ASEC Report 9월

® ASEC Report

2005. 10

I.9월 AhnLab 악성코드 동향	3
(1) 악성코드 피해동향	3
(2) 9월 국내 신종 (변형) 악성 코드 발견 동향	8
II. 9월 AhnLab 스파이웨어 동향	15
III. 9월 시큐리티 동향	17
IV. 9월 세계 동향	20
(1) 일본 악성코드 동향	20
(2) 중국 악성코드 동향	23
(3) 세계 악성코드 동향	27
V. 이달의 ASEC 컬럼 - 악성코드 재실행 기법	29

안철수연구소의 시큐리티대응센터(AhnLab Security E-response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

SUMMARY

악성코드로 인한 피해는 올 상반기에 상승세를 보이다가 7월부터 감소세를 나타내기 시작하여 9월에 이르러 2005년 최저치를 기록했다. 이러한 전체적인 감소에도 불구하고 9월 동향 특징으로 Win32/Netsky, Win32/Mytob등의 변형 Mass Mailer 피해가 증가하여 하였다. 피해 신고 된 악성코드 top 10의 감염유형별 현황을 살펴보면 네트워크 취약점을 이용한 것과 메일을 이용한 것의 비율이 4:6의 비율로 전월에 비하여 메일을 이용한 감염유형이 증가하였다. 9월은 8월과 비교하여 전체적으로 신종 및 변형에 대한 악성코드건수가 조금 줄어 들었다. 가장 많은 수를 자치하는 트로이목마와 웜 유형에서 다소 줄어든게 그 원인이다. 특히 악성 IRCBot 웜 경우 국내고객으로부터 접수 받은 샘플수는 46건에 불과 하였다. 이는 V3의 실행압축해제, 제너릭, 휴리스틱 진단기능(Unpacking, Generic, Heuristic Detection)의 향상의 결과로도 볼 수 있겠다. 피해신고와 마찬가지로 트로이목마의 발견이 강세를 보이고 있어, 전체 발견된 신종(변형) 중 52%를 트로이목마가 차지하고 있다. 이번달에 발견된 신종 악성코드 중에서 윈도우 OS 에서는 별다른 이슈가 없었으나, 심비안 OS 에서 동작되는 악성코드 몇 개가 관심을 받았다. 디바이스를 직접적으로 공격하는 형태들이며 이전에 알려진 Skulls 처럼 심비안 OS 부팅에 관련 시스템 파일에 피해를 주어 정상적인 부팅을 방해하거나 메모리 카드 또는 윈도우 OS 에 피해를 주는 형태들이 발견 되었다.

8월에 비해 상대적으로 애드웨어(adware)의 비율이 줄어들었지만 이는 애드웨어의 감소가 아닌, 스파이웨어(spyware)와 다운로더(downloader)가 증가했기 때문이다. 특히 감소 추세를 보이던 다운로더가 다시 증가함으로 인해 다운로더가 설치하는 스파이웨어와 애드웨어가 증가한 것으로 추정된다.

9월에는 MS에서 정기 보안 패치를 발표하지 않았으나, 몇몇 IE 취약점이 발표된 상태이다. 또한 SQL injection 공격을 이용하여 유명 사이트를 해킹한 다음, 트로이목마를 배포하는 사건이 지속적으로 발생하고 있으며, 행자부에 대한 국감에서 전자 정부에서 발급한 민원 서류 위/변조 가능성이 문제가 되어 민원 서류 발급이 중단되는 사건이 있었다.

9월 세계 악성코드 동향은 한국과 중국을 중심으로는, 중국에서는 여전히 트로이목마 류의 악성코드에 의한 감염 피해가 증가하고 있으며, 전체 분포에서도 크게 차지하고 있다. 그리고 인접한 한국 역시 중국발로 여겨지는 해킹 사고와 트로이목마 대량 유포 사고가 발생하는 유사한 형태를 띄고 있다. 그러나 일본의 경우에는 오히려 기존에 알려진 메일로 전파되는 넷 스카이 웜과 베이글 웜에 대한 감염 피해가 큰 것으로 분석하고 있다. 그러나 일본의 경우에는 악성코드에 직접적인 피해보다 중국으로부터 유입되는 서비스 거부 공격 등의 일련 해킹 시도에 대한 우려가 더 커지고 있는 것으로 보여지고 있다. 일본의 악성코드 동향과 유사하게 유럽 지역 역시 메일 전파되는 넷 스카이 웜과 자피 웜에 대한 감염 피해가 큰 것으로 보고 되고 있으며 이와 더불어 심비안 운영체제에서 작동하는 모바일 악성코드도 꾸준히 등장하고 있는 실정이다.

이달의 ASEC 컬럼에서는 최근에 실행과 동시에 자신의 동작상태를 감시하여 비정상적인 종료가 발생할 경우 재실행하는 기능을 가지고 있는 악성코드들이 종종 발견되고 있다. 이러한 기능은 악성코드가 자신을 보호하기 위해 사용하는 방법으로 현재 다양한 기법들이 사용되고 있다. 만약, 이러한 증상을 나타내는 악성코드에 감염될 경우, 사용자는 해당 악성 프로세스를 수동으로 삭제할 수 없으므로 적절한 대응을 할 수 없게 된다. 현재까지 이러한 종류의 악성코드가 빈번하게 발생하고 있지는 않지만, 웜(worm)과 같이 전파력이 높은 악성코드에서 이러한 기법이 사용될 경우, 사용자에게 큰 피해를 줄 수 있을 것으로 예상된다. 따라서, 현재까지 접수된 샘플 중 이러한 증상을 나타내는 악성코드들을 유형별로 분류하여 각각의 증상들을 살펴보고 나아가 적절한 대처방법을 제시한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

I. 9월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자 : 조성준 주임 연구원(sjcho@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	153	12.6%
2	-	Win32/Maslan.C	109	9.0%
3	↑5	Win32/Sasser.worm.15872	38	3.1%
4	↑7	Win32/Zotob.worm.31744	32	2.6%
5	↓6	Win32/Tenga.3666	31	2.6%
6	new	Win32/Mytob.worm.48766.C	27	2.2%
7	new	Win32/Parite	24	2.0%
8	new	Win32/Netsky.worm.25352	21	1.7%
9	↓8	Win32/Mytob.worm.59006	16	1.3%
10	new	Win32/Mytob.worm.47674	14	1.2%
		기타	747	61.6%
합			1,212	100

[표1] 2005년 9월 악성코드 피해 Top 10

9월 악성코드 피해 동향

악성코드로 인한 피해는 올 상반기에 상승세를 보이다가 7월부터 감소세를 나타내기 시작하여 9월에 이르러 2005년 최저치를 기록했다. 이러한 전체적인 감소에도 불구하고 9월 동향 특징으로 Win32/Netsky, Win32/Mytob등의 변형 Mass Mailer 피해가 증가하여 Top 10위 안에 무려 5개나 차지하였고, [표 1]에서와 같이 새로 진입한 악성코드 중 3개는 Mass Mailer류의 악성코드이다.

새로 순위에 진입한 악성코드 중 Win32/Parite는 바이러스로 분류되지만, 네트워크 공유폴더로 확산되는 기능을 가지고 있다.

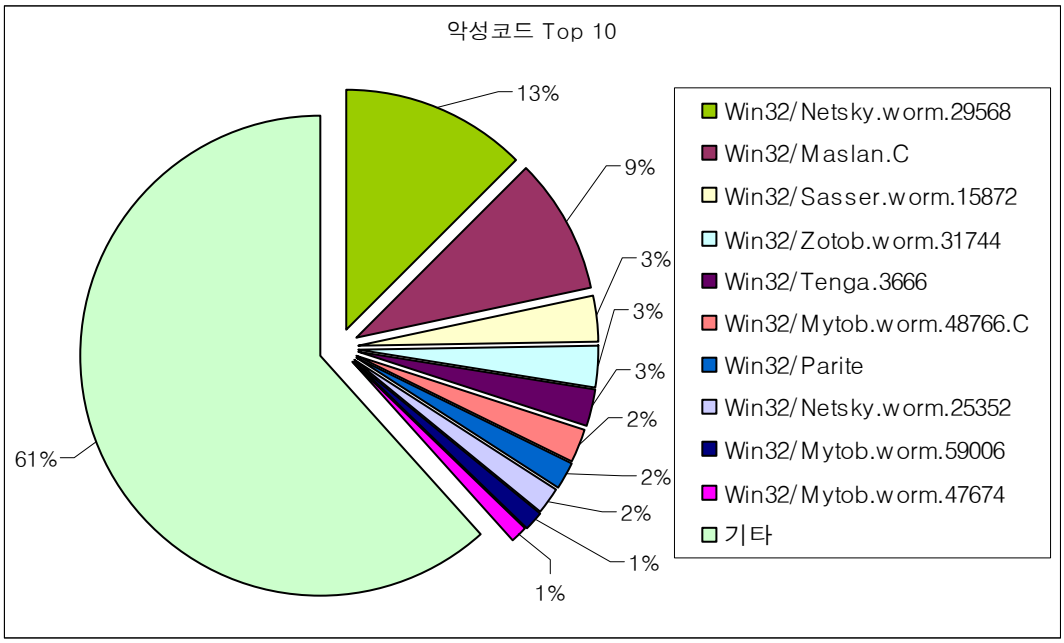
Win32/Parite는 2002년 8월에 국내에서 처음으로 발견되었으며, 네트워크를 스캔하여 스스로 감염대상을 찾아 읽기/쓰기 공유된 폴더에 접근을 시도하며 *.exe, *.scr 파일을 찾아 감염시킨다. Upx 형식으로 압축된 실행 가능한 *.TMP (랜덤한 파일명과 확장자 TMP) 파일을 생성하여 예전 Win32/Nimda와 유사하게 실행중인 EXPLORER 에 모듈로 붙어 바이러스가 계속 실행된다.

해당 바이러스의 특성상 네트워크를 따라 다니며 감염되기 때문에 한대의 PC라도 감염된 채 남아 있으면 치료 후에도 재감염 될 수 있으므로 치료 시에는 반드시 공유된 폴더를 해제해야 하며, 공유가 반드시 필요하다면 되도록 읽기 가능으로만 공유를 해야 한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

9월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.

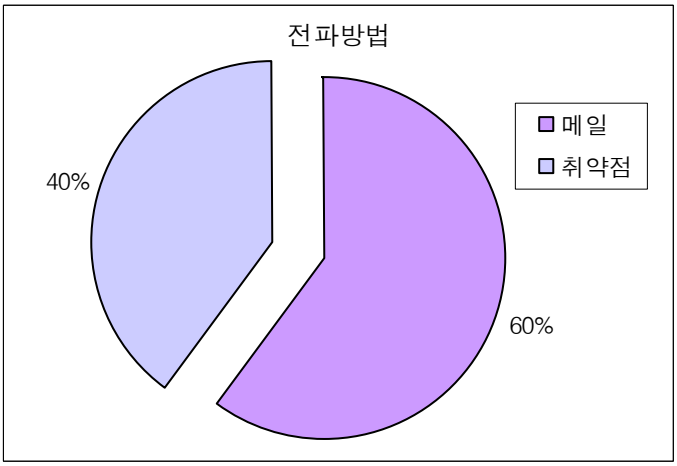


[그림1] 2005년 9월 악성코드 피해 Top 10

지난달 3, 4위를 차지 하던 정보 유출시도용 Trojan인 Win-Trojan/Hanghack.44032, Win-Trojan/Xema.31744.B는 순위에서 밀려 났으며, 이는 웹 서버 관리자의 보안의식 강화에 따른 취약 웹사이트 감소로 추정된다. 해당 정보 유출시도용 Trojan은 순위에는 들지 못하였지만 변종의 수는 더욱 늘어나 50여종에 이른다.

9월 악성코드 Top 10 전파방법별 현황

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

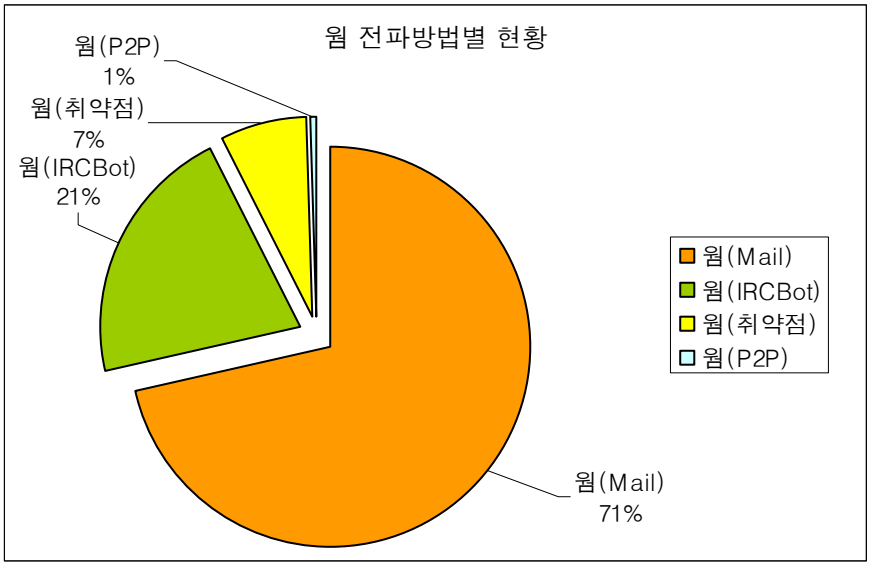


[그림2] 악성코드 Top 10의 전파 방법별 현황

Copyright © AhnLab Inc,. All Rights Reserved.

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

[그림2]에서와 같이 피해순위 Top 10에 랭크된 악성코드의 60%가 메일을 이용하여 전파되고 있다. 지난 8월에 비해 메일 전파도가 10%가 증가하고 네트워크와 운영체제 취약점을 이용한 전파가 10%가 감소하였다. 메일을 이용하여 전파되는 악성코드에 대해 사용자는 아는 사람에게서 받은 메일이라 해도 메일을 열 때에는 항상 주의해야 하고, 특히 제목이나 본문 내용이 영문인 메일을 받으면 첨부 파일은 열지 말고 V3로 우선 검사한 후 실행하는 습관을 가져야 하며, 주기적으로 윈도우 업데이트를 통하여 보안패치도 적용해야 한다.



[그림3] 웜의 전파방법별 현황

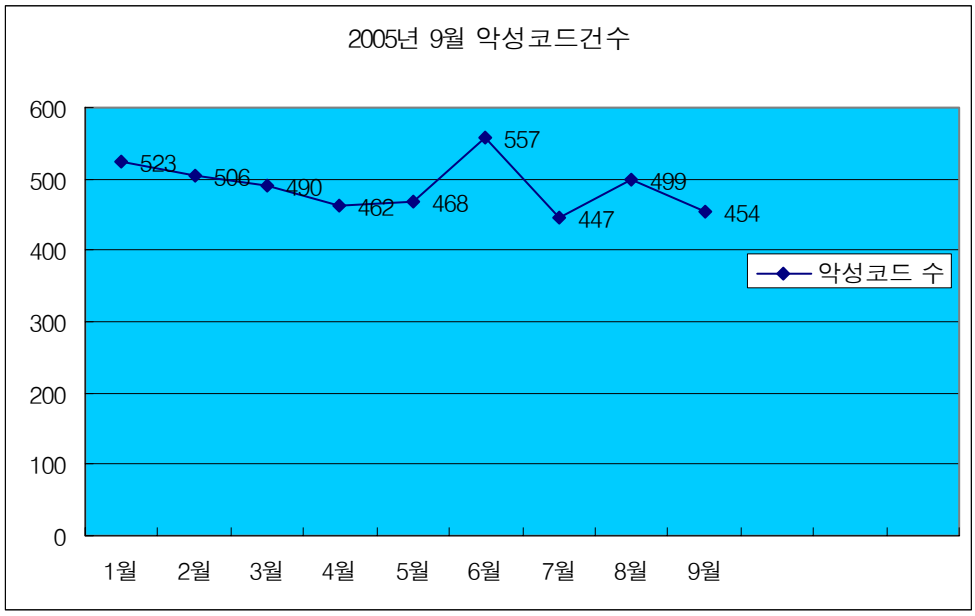
[그림3]은 9월에 피해 신고된 웜의 전파방법에 대한 현황으로, 이메일(Mail)과 인터넷 채팅(IRC)이 92% 차지하는 것으로 집계되었다. 따라서, 이메일을 확인하거나 인터넷 채팅(IRC) 방에 접속할 때는 최신 엔진으로 업데이트된 백신제품의 실시간 기능을 항상 켜두고 사용하기를 권장한다. 또, 취약점을 이용한 전파는 1%가 줄고, P2P를 이용한 전파가 1% 증가하였다.

월별 피해신고 악성코드 건수 현황

9월에 피해 신고된 악성코드는 454개이며, 지난 8월에 비해 40건 정도 감소하였다. 이는 Trojan인 Win-Trojan/Hanghack.44032, Win-Trojan/Xema.31744.B가 순위에서 밀려 난 것에서 알 수 있듯이 확산도가 큰 웹사이트 해킹 유포되는 트로이목마의 피해 감소로 인한 것으로 보인다.

Copyright © AhnLab Inc,. All Rights Reserved.

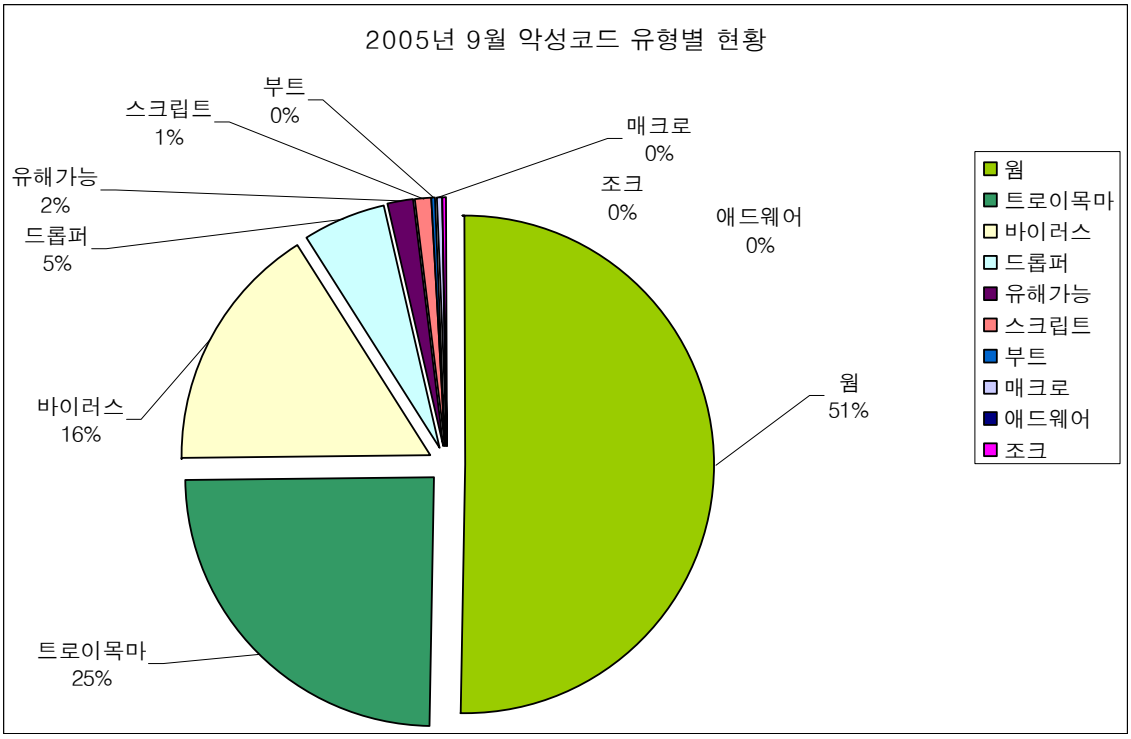
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림4] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

9월에는 8월에 비해 웜이 4% 가량 증가한 반면, 트로이목마는 5% 가량 줄어 들었다. 트로이목마 변종 수는 늘어 났지만, 전체 피해 비율은 줄어 들었다. 이는 보안패치설치 및 백신의

Copyright © AhnLab Inc,. All Rights Reserved.

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

최신엔진 업데이트 등 일반 사용자 보안 의식 발전 결과로 보여진다.

바이러스비율이 꾸준히 증가하여 지난 8월에 비해 현재 1% 증가하였다. 이는 바이러스이지만 메일을 이용한 유포기능을 갖고 있는 Win32/Maslan.C와 공유폴더 및 Netbios를 이용한 유포기능을 갖고 있는 Win32/Tenga.3666, Win32/Parite의 피해 신고 증가가 원인이다.

9월 동향 특징으로 Win32/Netsky, Win32/Mytob등의 변형 Mass Mailer 피해가 증가하여 Top 10위 안에 무려 5개나 차지한 부분에서 확인하였다. 새로 순위에 진입한 악성코드 중 Win32/Parite는 바이러스로 분류되지만, 네트워크 공유폴더로 확산되는 기능을 가지고 있다.

이를 예방을 위해서는 우선 전산 관리자들은 주기적으로 웹 서버 등 중요 시스템의 보안 취약점을 사전에 체크하고, 최신 패치 프로그램을 설치하는 것이 중요하며, 일반 사용자들은 이런 종류의 피해를 막기 위해서 최신 보안패치와 함께 최신 버전의 백신프로그램으로 실시간 감시 기능을 사용하는 습관이 필요하다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

(2) 9월 국내 신종 (변형) 악성 코드 발견 동향

* 작성자: 정진성 주임 연구원 (jsjung@ahnlab.com)

9월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비 윈도우	합계
58	116	30	7	0	1	0	0	13	0	225

[표1] 2005년 8월 유형별 신종 (변형) 악성코드 발견현황

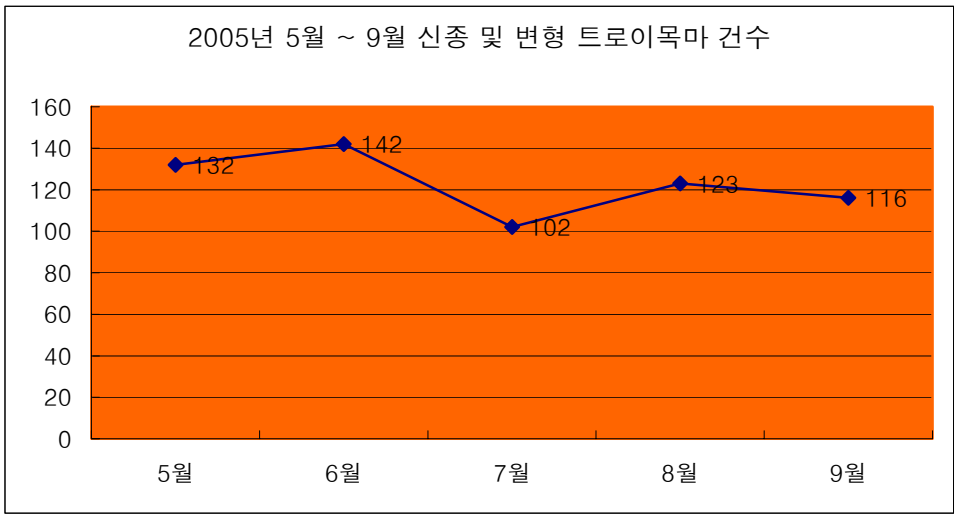
9월은 8월과 비교하여 전체적으로 신종 및 변형에 대한 악성코드건수가 조금 줄어 들었다. 가장 많은 수를 자치하는 트로이목마와 웜 유형에서 다소 줄어든게 그 원인이다. 특히 악성 IRCBot 웜 경우 국내고객으로부터 접수 받은 샘플수는 46건에 불과 하였다. 이는 V3의 실행압축해제, 제너릭, 휴리스틱 진단기능(Unpacking, Generic, Heuristic Detection)의 향상의 결과로도 볼 수 있겠다. 하지만 이 숫자가 항상 감소하는 것은 아니다. 다른 악성코드도 마찬가지이겠지만 악성 IRCBot 제작자들은 안티 바이러스로부터 진단을 회피하기 위한 여러 방법을 사용한다. 예로 컴파일한 바이너리에 새로운 실행압축을 하거나 소스를 변경하여 위와 같은 진단방법을 회피하기 때문이다. 악성 IRCBot 소스는 인터넷 게시판, IRC 등의 커뮤니티를 통해서 교환되거나 돈을 주고 살수도 있다. 따라서 프로그래밍에 정통한 한명의 제작자가 자신의 소스를 공개하면 다른 누군가 이를 수정하거나 또는 그대로 컴파일하고 안티 바이러스가 지원하지 않는 실행압축을 하면 또 하나의 변형이 제작 되어진다. 이와 같은 식을 반복하여 악성 IRCBot 은 끊임없이 제작과 배포를 반복한다. 따라서 대부분의 안티 바이러스 업체들이 이러한 점을 놓치지 않고 실행압축해제, 제너릭, 휴리스틱 진단기능(Unpacking, Generic, Heuristic Detection)의 향상 연구와 이를 반영한 엔진개발에 많은 투자를 하고 있다.

다음은 9월까지 최근 5개월간의 국내고객으로부터 접수된 트로이목마의 샘플수를 조사해보았다. 트로이목마가 차지하는 악성코드의 비율은 과반수를 넘어선지 오래되었다. 주로 발견되었던 트로이목마는 다음과 같다.

- Win-Trojan/BackDoor
- Win-Trojan/Downloader
- Win-Trojan/Bagle
- Win-Trojan/LineageHack
- Win-Trojan/PcClient
- Win-Trojan/Swizzor

Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림1] 최근 5개월간 트로이목마 발견건수

9월에 발견된 트로이목마들은 크게 전형적인 백도어 증상을 가진 것과 특정 호스트로부터 다른 악성코드를 다운로드하는 것으로 나누어진다. 전자는 아주 일반적 형태라 할 수 있겠다. 특정 호스트로부터 파일을 다운로드 받아오는 형태는 최근 악성코드 경향을 잘 반영한 형태라 할 수 있다. 이러한 형태는 트로이목마에서 주로 많이 확인 되고 있으며 이는 "악성코드의 모듈화" 를 뜻한다. 즉, 이러한 악성코드의 처음형태는 다른 호스트에서 파일을 다운로드하는 형태에 불과하였으나 해당 파일을 받아서 그 악의적인 기능을 확장하는 형태를 가지고 있다.

대표적인 악성코드가 위에서 소개된 Win-Trojan/Bagle(이하 베이글 트로이목마)을 들 수가 있다. 초기 증상은 안티 바이러스를 비롯한 보안 관련 프로그램들을 무력화하고 이후 특정 호스트에 업로드된 악성코드를 다운로드하여 실행한다. 다운로드된 악성코드 역시 안티 바이러스의 호스트나 보안 관련 웹 사이트에 감염 시스템의 접속을 방해하는 증상을 가지고 있다. 이렇게 되면 감염된 해당 시스템은 완전 무방비 상태로 노출되어 있으므로 악의적인 목적을 가진 사용자가 접근할 수도 있고 다른 시스템의 명령을 받아 수행할 수도 있게 되어 버린다.

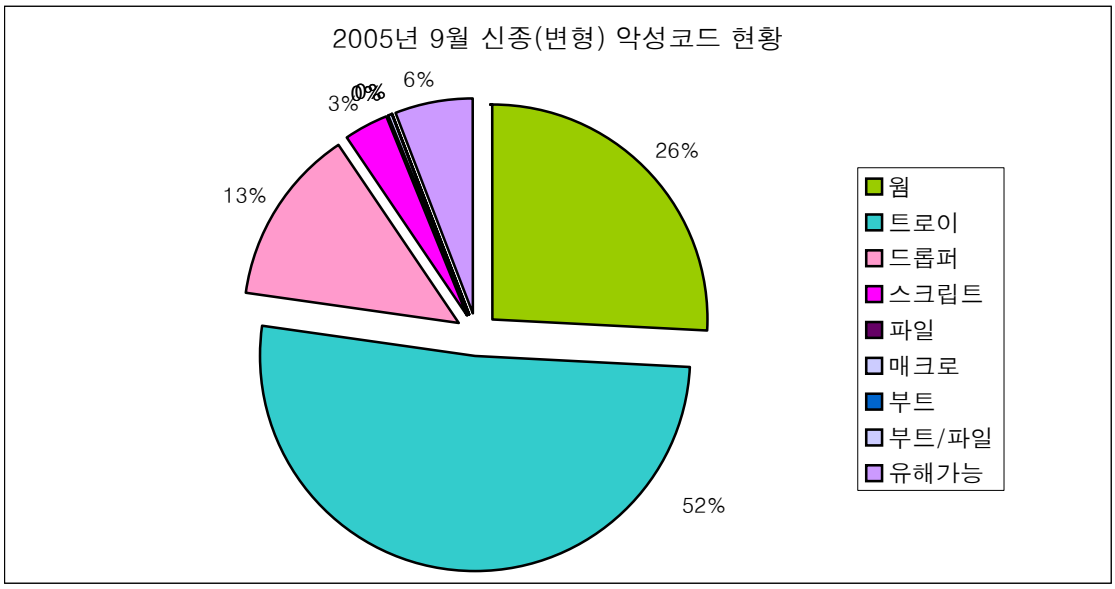
이렇듯 처음 형태의 악성코드는 매우 단순한 기능을 가지지만 이후 제작자가 업로드한 파일에 따라 다양한 악의적인 증상을 가진 악성코드로 변할 수 있게 된다. 또한 베이글 제작자는 안티 바이러스로부터 진단을 회피할 목적으로 기존에 알려져서 안티 바이러스에서 처리하는 실행 압축 툴을 변형하여 계속 사용하고 있으며 최근에는 압축 알고리즘 마저 일부 변형하여 사용하고 있다. 이러한 악성코드의 대응은 엔진을 항상 최신으로 유지 하는 것이 제일 현명한 방법이 될 수 있겠다.

[그림2]는 9월 신종(변형)악성코드의 비율을 나타낸 것이다. 위에서 언급한 것처럼 트로이

Copyright © AhnLab Inc,. All Rights Reserved.

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

목마의 비율이 전체의 반을 이미 넘어선 상태이다.



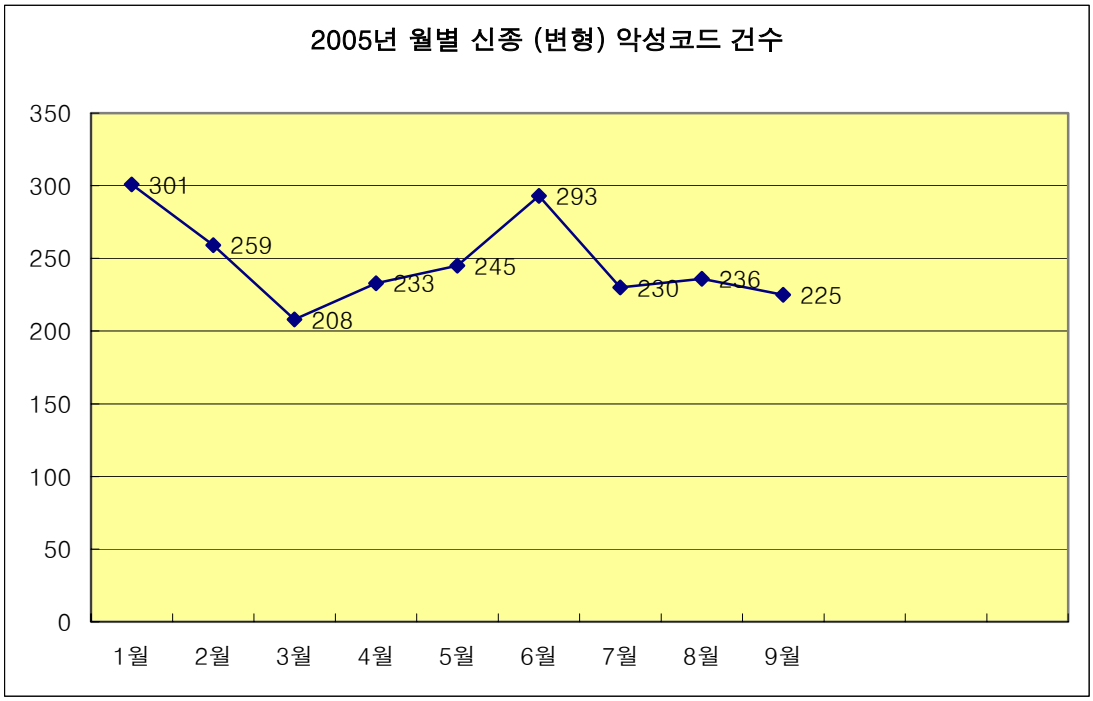
[그림2]2005년 9월 신종(변형) 악성코드 비율

[그림 3]은 국내고객으로부터 접수된 신종 및 변형의 악성코드의 건수를 나타내고 있다. 이는 단지 국내 고객들로부터만 접수 받은 샘플이다. 9월은 최근 5개월과 비교해서 낮은 샘플 건수를 보여주고 있다. 하지만 이는 해외에서 이슈가 되었던 악성코드나 중국, 일본 지사에서 접수된 샘플은 제외된 것이여서 실제로는 이보다 더 많은 샘플이 엔진에 추가된다. 9월달에는 약 3,000개가 넘은 악성코드가 엔진에 추가 되었다. 이중 국내 접수된 악성 IRCBot 웜만 추려본다면 219건 정도이다. 이는 해외에서 이슈된 악성 IRCBot 은 제외한 수이고 앞서 말한 것처럼 국내접수 샘플에 다른 경로로 접수되어 국내에서 발견된 악성 IRCBot 웜의 수이다.

과거 오랜 악성코드 동향을 보면 엄청난 피해를 입힌 악성코드가 멸종에 가까울 정도로 잠잠해질 때가 있다. 하지만 불규칙한 편차를 지닌 악성 IRCBot의 국내 접수 샘플 수는 실제로 악성코드의 수가 줄어들고 있는 것이 아니므로 이를 간과해서는 안 될 것이다.

Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림3]2005년 월별 신종(변형) 악성코드 발견 현황

9월 주요 신종(변형) 악성코드 정리

MS05-039 관련 취약점과 이를 이용한 웜 (이메일 웜, 네트워크 웜)들이 기승을 부렸다. 이 취약점은 앞으로도 제작되는 악성코드에 계속 이용될 것으로 보인다.

이번달은 윈도우 OS 에서는 별다른 이슈가 없었으나, 심비안 OS 에서 동작되는 악성코드 몇 개가 관심을 받았다. 디바이스를 직접적으로 공격하는 형태들이며 이전에 알려진 Skulls 처럼 심비안 OS 부팅에 관련 시스템 파일에 피해를 주어 정상적인 부팅을 방해하거나 메모리 카드 또는 윈도우 OS 에 피해를 주는 형태들이 발견 되었다.

휴대폰 악성코드는 자신의 전파방법을 Bluetooth 에서 MMS (Multimedia Messaging Service)로 이동하여 국지적인 한계를 벗어 났으며 이제는 휴대폰과 연결될 수 있는 다른 운영체제나 시스템도 감염대상으로 포함하고 있다는 점에서 문제시 되고 있으며 아직은 광범위하게 문제를 일으키지 않았던 이 악성코드들도 조만간 우리에게 큰 위협으로 다가올 날이 멀지 않는 것 같다.

이슈가 되었던 이번달의 악성코드는 다음과 같다.

▶ Win32/Wullik.worm

이 악성코드는 2003년도에 발견된 구종의 이메일 웜이다. 매스컴을 통해서 다시 알려졌는데

Copyright © AhnLab Inc,. All Rights Reserved.

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

그 이유는 MP3 플레이어내에 이 웜 파일이 존재 했다는 이유 때문이다. 이 웜의 증상은 아웃룩 주소록의 사람들에게 자신이 첨부된 메일을 보내며 공유폴더에 자신의 복사본을 생성한다. 따라서 MP3 플레이어에서 필요한 프로그램을 넣어둔 폴더에 이 웜이 복사되었고 이를 모르고 그대로 제품을 생산한 것으로 추정할 수 있다. 아직 윈도우 악성코드가 인터넷 연결이 가능한 가전제품에 감염된 사례를 보고 받은 적은 없으나 다가올 유비쿼터스 시대에는 아마도 이런 일은 흔하게 발생하지 않을까 예측된다.

▶ 심비안 OS 에서 동작하는 악성코드 3종 (휴대폰 악성코드)

국외 휴대폰의 보편적인 OS 인 심비안에서 동작하는 휴대폰 악성코드가 계속 발견되고 있다. 한국은 해당 지역과 휴대폰이 다른 형태라 아직까지는 안전지대에 속해 있다. 하지만 이 OS 를 탑재한 모바일 기기들이 계속적으로 나오면서 더 이상 간과해서는 안 될 것이다. 일부 안티 바이러스 업체에서 Doomboot와 Cardtrap, Cardblock 이라고 명명된 악성코드를 발견, 보고했다. 이 악성코드의 특징은 디바이스나 윈도우 시스템을 직접 타켓으로 노리고 있다.

Doombot는 자신이 실행될 때 손상된 시스템 파일을 설치하여 이후 휴대폰을 재부팅 했을 때 제대로 부팅되지 않도록 하는 증상이 있다. Cardtrap 은 메모리 카드에 윈도우 악성코드 2 개의 설치해두고 사용자가 메모리 카드를 컴퓨터에 연결했을 때 악성코드가 동작하도록 하는 방식을 가지고 있으나 다행히도 많은 사용자들이 사용하는 윈도우 2000, XP 에서는 이 방법으로는 실행되지는 않았다. Cardblock 은 메모리 카드에 암호를 설정하여 휴대폰 및 다른 디바이스에서도 이를 접근할 수 없도록 해둔다. 암호를 해제하는 방법은 본 글을 작성할 때까지도 알려지지 않았다.

윈도우 악성코드에서 다른 기기로의 악성코드 전파는 충분히 예상된 것 이였다. 하지만 휴대폰에서 윈도우로 이어지는 전파는 미처 예상하지 못한 방법이였다. 물론 그 방법이 매우 단순한 형태이기는 하지만 이것은 디바이스 및 시스템 자체를 못쓰게 한다는 점에서 피해가 매우 크다고 할 수 있겠다. 아직 이 악성코드들이 광범위하게 전파되지는 않았지만 이러한 악성코드의 출현은 이 기반의 핸드폰을 사용하는 지역에서는 우려스러운 일이 아닐 수 없다.

▶ 가짜 Flash Player v8 설치를 유도하는 웹 사이트

한국 내 보안이 취약한 웹 사이트들이 해킹을 당하고 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마가 설치되는 것이 점점 극에 달하고 있다. 이러한 방법은 웹 서버 또는 SQL 관련 취약점을 이용하여 Root 권한을 획득하고 웹 페이지를 변조하여 트로이목마의 다운로드를 유도하도록 해두는 방식이다. 그런데 최근에는 SWF 파일 재생으로 유명하고, 이를 웹 브라우저에서 지원하도록 만든 Flash Player v8을 가장하여 해당 ActiveX를 다운로드하는 트로이목마가 설치되도록 하는 형태가 발견 되었다. 이는 9월초부터 실제로 Flash Player v8로 업데이트한 사이트가 많아져 이를 노려 가짜 ActiveX를 만들어 트로이목마 유포한 것으로 보인다. 이 가짜 Flash Player v8 은 인증 사인이 없으므로 진짜 ActiveX와 쉽게 구별

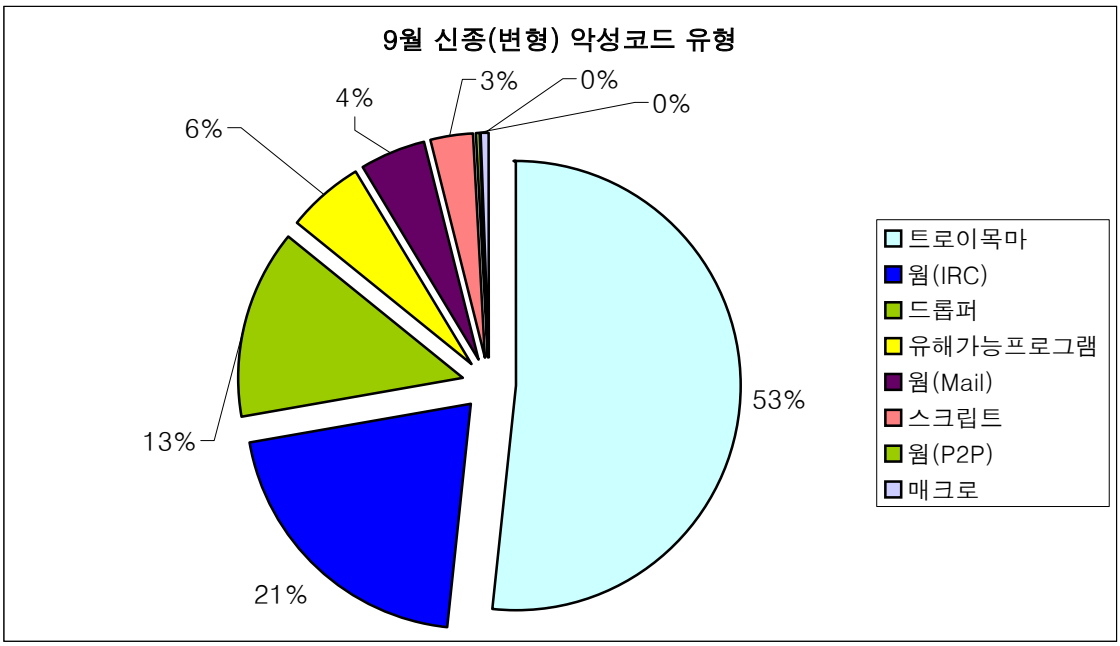
Copyright © AhnLab Inc,. All Rights Reserved.

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

된다.

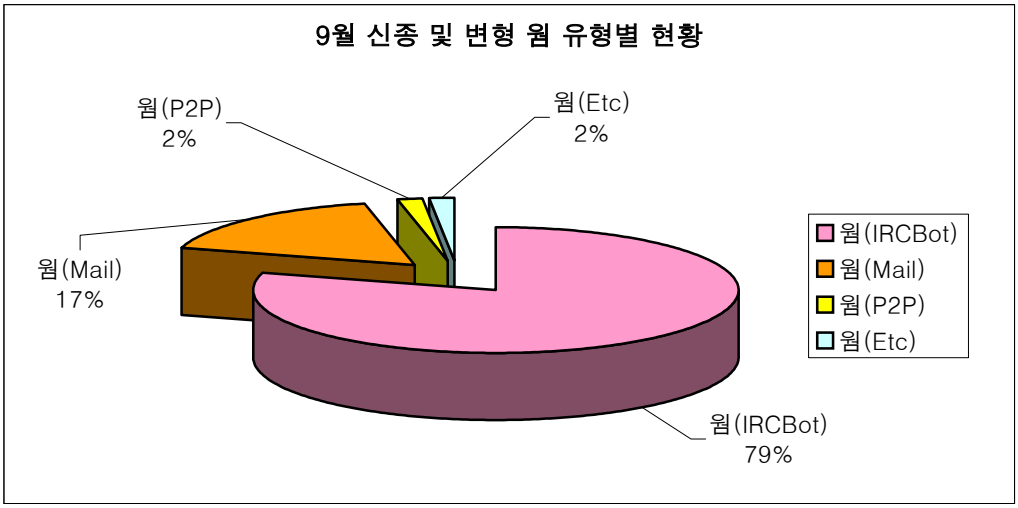
이외에도 Bagle 웜과 트로이목마 변형이 기승을 부렸는데 이 때문에 하루에도 수개의 변형이 쏟아져 바쁜 엔진 업데이트가 이루어진 적도 있었다.

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



[그림4] 9월 신종 (변형) 악성코드 유형별 현황

이중 광범위하게 타격을 줄 수 있는 웜 유형에 대하여 다시 상세 분류해보았다. 다음과 같다.



[그림5] 9월 신종 및 변형 웜 유형별 현황

Copyright © AhnLab Inc,. All Rights Reserved.

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

그 동안 한 두건씩 피해문의가 있었던 메신저 관련 웜은 이번 달의 경우 국내고객으로부터 한 건도 접수되지 않았다. P2P 웜은 일본지역에서 발견된 Antinny 웜 이다. 기타 웜으로 분류된 것은 국내 고객으로부터 접수되었으나 실제로 피해는 없었던 도스에서 동작하는 웜 이였다.

이번 달의 주요 이슈는 전체적으로 Bagle 웜과 트로이목마에 대한 잦은 변형의 발견과 대응 그리고 디바이스를 노리는 국외에서 보고된 심비안 OS 악성코드 등으로 정리할 수 있다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

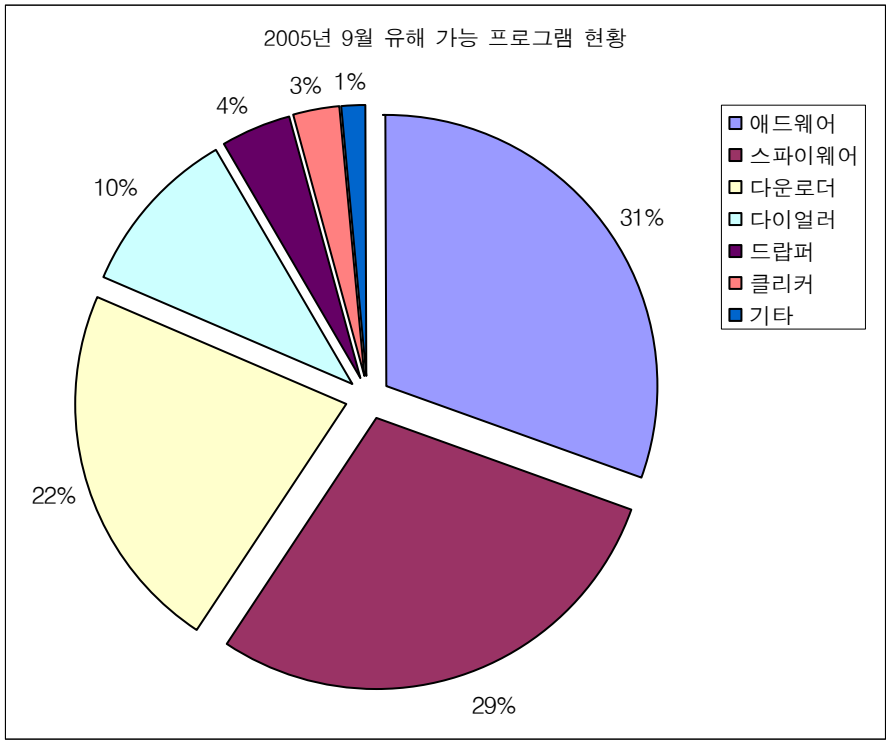
II. 9월 AhnLab 스파이웨어 동향

작성자 : 박시준 연구원(sjpark@ahnlab.com)

9월 한달 동안 접수된 신종(변형) 유해 가능 프로그램 건수는 [표1], [그림1]과 같다.

애드웨어	스파이웨어	다운로더	다이얼러	드랍퍼	클리커	기타	합계
293	275	213	96	42	25	14	958

[표1] 2005년 9월 유형별 신종(변형) 유해 가능 프로그램 발견 현황



[그림1] 2005년 9월 발견된 유해 가능 프로그램 비율

2005년 8월에 비해 상대적으로 애드웨어(adware)의 비율이 줄어든 것을 볼 수 있다. 하지만 이는 애드웨어의 감소가 아닌, 스파이웨어(spyware)와 다운로더(downloader)가 증가했기 때문이다. 특히 감소 추세를 보이던 다운로더가 다시 증가함으로 인해 다운로더가 설치하는 스파이웨어와 애드웨어가 증가해 전체적으로 발견된 유해 가능 프로그램의 숫자가 크게 늘어난 결과를 보였다.

은폐형 스파이웨어의 증가

9월엔 특히 Win-Spyware/Transponder.Nail, Win-Adware/BetterInternet, Win-Clicker/SPAlert에 대한 감염 신고가 많았는데, 이는 Win-Dropper/Vidro라는 은폐형 스파이

Copyright © AhnLab Inc,. All Rights Reserved.

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

웨어와 일반적인 방법으로 치료가 어려운 Win-Spyware/Pakes가 해당 스파이웨어를 지속적으로 설치해서 발생한 현상이다. 또한 지속적으로 변형이 발견되고 있는 Win-Adware/ToolBar.EliteBar의 경우도 은폐형 기법을 사용하여 일반적인 방법으로 진단 및 치료가 매우 어렵다. 현재 이를 진단하고 치료하는 안티 스파이웨어 제품이 거의 없기 때문에 이에 관한 피해 사례는 당분간은 계속 이어질 전망이다.

정상적인 프로그램과 서비스를 악용하는 스파이웨어의 증가

최근 스파이웨어 중 눈에 띄는 점은 정상적인 프로그램이나 서비스를 악용하는 스파이웨어가 늘어나고 있다는 것이다. 대표적인 예로 Spyware/StartPage.30720를 들 수 있는데, IP주소를 얻어오는 과정에서 DNS 쿼리에 앞서 HOSTS 파일의 내용을 먼저 참조해 검색하고자 하는 도메인네임에 관한 정보가 있으면 DNS 쿼리를 하지 않는다는 점을 악용한 사례로 구글 툴바(Google Toolbar), MSN, Yahoo의 검색 결과를 스파이웨어에서 사용하는 사이트로 리다이렉션(redirection) 시키도록 HOSTS의 내용을 변경한다. 따라서 사용자는 원인도 모르고 원하는 검색 결과가 아닌 스파이웨어가 지정한 사이트로 접속하게 된다.

또한 국내 유명 온라인 게임의 계정 정보를 외부로 유출하는 스파이웨어인 Win-Spyware/PWS.Lineage.50932의 경우 윈도우의 정상적인 서비스인 IPv6 Helper Service를 스파이웨어로 바꿔 실행시키는 사례로, 이 스파이웨어가 설치될 경우 IPv6를 IPv4로 변환해주는 서비스가 동작하는 것이 아니라 Win-Spyware/PWS.Lineage.50932 스파이웨어가 실행 된다. 따라서 사용자는 사용하고자 하는 윈도우 서비스를 사용하지 못하는 대신 사용자의 계정 정보를 외부로 유출하는 스파이웨어가 실행되어 2중의 피해를 입을 수 있으며 해당 서비스를 다시 이용하기 위해서는 스파이웨어의 제거는 물론 사용하고자 하는 서비스를 재설치 해야 하는 번거로움을 겪어야 한다.

연이은 대형 포탈 사이트의 해킹

8월에도 종종 보고되었던 국내 대형 포탈 사이트에 대한 해킹은 9월 달에도 역시 이어졌다. 주로 중국에서 국내 유명 온라인 게임의 계정 정보를 유출시키기 위한 스파이웨어를 설치하는 코드를 삽입하는 형태로 상당수가 사용하는 유명 대형 포탈 사이트들이 해킹되어 그 피해자가 적지 않을 것으로 예상되며 이런 현상이 지속된다면 그 피해는 더욱 커질 수 밖에 없을 것이다. 따라서 각 회사의 보안 관리자들의 각별한 주의와 다각도의 노력이 더욱더 필요하며 개인 사용자의 경우도 자신의 개인 정보가 외부로 유출되지 않도록 각별한 주의가 필요하다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

III. 9월 시큐리티 동향

작성자 : ASEC 분석2팀 / 이정형 주임연구원(jungh@ahnlab.com)

1. 주요 보안 이슈

9월에는 매월 둘째 주 화요일에 발표하는 마이크로소프트사의 정기 보안패치가 발표되지 않았는데, 마이크로소프트사에서는 해당 보안 패치의 품질향상을 위해 좀 더 많은 테스트 진행을 이유로 10월로 연기한다고 공고하였다.

Internet Explorer 6의 새로운 보안취약점이 security-protocols 에서 활동중인 Tom Ferris 에 의해 발견되었다. 이번 취약점을 통해 사용자 동의 없이 악의적인 프로그램이 설치될 수 있고, 악성코드나 스파이웨어 등에서 이용될 수 있다. 마이크로소프트사에서는 현재 해당 취약점을 조사 중에 있으며, 아직까지 보안패치는 발표되지 않았다. 현재 공격코드는 공개되지 않았지만 주의가 요망된다.

또 다른 보안 이슈로 Cisco Router 의 운영체제인 IOS 에서 Authentication Proxy for FTP/Telnet Buffer Overflow 가 발견이 되었다. 해당 프록시에 buffer overflow가 존재를 하여, 악의적인 사용자가 이 취약점을 이용할 경우 Router를 장악을 할 수도 있게 된다. 네트워크 장비의 최전방에 있는 Router 의 보안에도 주의가 요구된다.

그 밖에 고려대 컴퓨터보안연구실의 이희조 교수가 주요 시스템 구축과 행사 진행을 총괄 담담하고, 안철수연구소가 시스템 지원 및 문제 출제 등 제반 지원을 담당한 지난 23일과 24일 양일간에 걸쳐 제 3회 카이스트-포항공대 학생대제전(일명'사이언스 워')의 해킹대회가 개최되었으며, 올해는 포항공대(12): 카이스트(7)로 포항공대가 승리하였다.

2. 국내 홈페이지 잇단 해킹

지난 1월에 국내 대량 홈페이지 변조사건을 시작으로, 연이은 국내 웹 서버들의 해킹 사건이 발생을 하였고, 또 지난 9월에는 중국해커의 소행으로 보이는 네티즌들이 많이 방문하는 국내의 유명 포털 사이트 뉴스페이지, 언론사 홈페이지, 공공기관, 음원 관련 사이트 등에 대한 해킹이 계속되고 있다.

해커는 해당 웹 페이지를 Internet Explorer 의 취약점을 이용한 트로이목마가 설치되게 변조하여 두고, 사용자들이 해당 웹 페이지를 방문하였을 때, 트로이목마가 사용자의 시스템에 설치되게 된다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

트로이목마는 감염된 시스템의 사용자가 특정 온라인 게임 웹 사이트를 접속 할 경우, 사용자 계정과 비밀번호를 후킹하여 특정 메일 주소로 전송을 시도하며. 제작자는 유출된 사용자 계정과 비밀번호를 이용하여 해당 계정이 보유하고 있는 사이버 머니 또는 아이템을 이용하여 금전적 이득을 취득하기 위해 제작한 것으로 추정된다.

공격을 당한 대다수의 시스템이 Windows NT계열 웹 서버이며, 웹 서버가 보안패치가 되어있음에도 불구하고, 대부분이 웹 어플리케이션 버그(SQL Injection등)로 공격을 당한 것으로 추정된다.

대부분의 웹 어플리케이션 취약점은 인자(Argumentation) 처리에서 쉘 메타캐릭터들을 제거시켜 주지 않아서 발생을 한다. 이러한 취약점을 완벽하게 해결을 하려면, 웹 어플리케이션을 제작하는 프로그래머들이 보안에 대한 마인드를 가지고, 코딩시에 주의를 해야 하며, 전체 웹 어플리케이션에 대한 보안검사(Audit)가 요구된다.

이 취약점에 대한 해결책은 다음과 같은 쉘 메타캐릭터들에 대해서 인자 처리시에 제거를 시켜주어야 한다.
쉘 메타캐릭터 문자들 - .;<>*|'&;$!#()[]{}:'"/^₩nWr
또한 지난 4월에 작성된 ASEC Monthly Report 에 보다 자세한 해결책이 제시되어 있다.

일반 사용자들은 윈도우 보안 패치 및 특히 Internet Explorer 에 대한 보안패치를 반드시 하고, 안티 바이러스 혹은 안티 스파이웨어 제품을 설치하여, 트로이목마의 감염을 방지할 수 있다.

3. 전자정부 인터넷 발급 위/변조 관련

지난 9월의 행정자치부 국정감사에서 모 국회의원이 지적한 것을 발단으로 전자정부 사이트에서 인터넷 민원서류 발급시 위/변조가 가능하다는 사실이 알려진 이후에, 현재는 전자정부사이트와 기관 사이트 등에서 각종 민원서류 신청이 모두 중지가 된 상황이다. 민원서류에는 개인정보 등이 들어가 있고 공신력을 가지는데, 악의적으로 위조가 된다면 개인정보를 이용한 여러 사건들이 발생을 할 수도 있게 된다.

이번에 문제가 된 것은 문서 출력시에 HTML 소스 변조나 이미지 변조 등이 가능한 것이 원인이 되었는데, 중요한 데이터의 위조와 변조의 문제는 인터넷 상을 떠나, 오프라인에서도 항상 문제를 가지고 있는 부분이다. 예를 들면, 관공서에서 발급된 특정 중요서류의 내용을 수정하거나, 이미지를 조작하는 위/변조 등은 예전부터 발생을 하고 있다. 이러한 문제가 인터넷을 통한 전자 정부에서도 가능하다는 것이 이슈가 된 것이다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

이러한 문제점을 보완하기 위해서는, 기본적으로 인터넷에서 민원서류 발급시 암호화, 일련번호 난수화, 특수 인쇄기법 등이 고려될 수도 있으며, 아울러 민원서류를 취급하는 곳에서도 위/변조를 식별할 수 있는 상호 보안 시스템이 필요한 것이다.

이에 대한 종합적인 대책은 현재 정부가 가능한 기술적·행정적·제도적 조치를 모두 취하겠다는 방침으로 다양한 방법을 고려중인 것으로 알려져 있다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

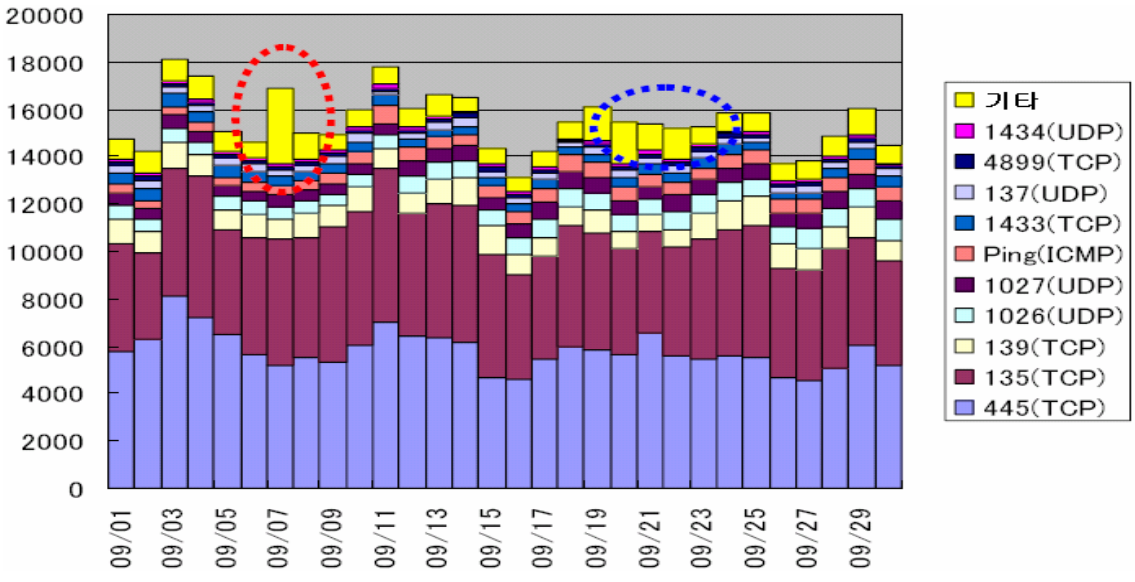
Ⅳ. 9월 세계 동향

9월 세계 악성코드 동향은 한국과 중국을 중심으로 한 악성코드 동향과 일본과 유럽 지역의 악성코드 동향이 상당히 다른 판도를 보이고 있다. 먼저 중국의 9월 악성코드 동향에서는 여전히 트로이목마 류의 악성코드에 의한 감염 피해가 증가하고 있으며, 전체 분포에서도 크게 차지하고 있다. 그리고 인접한 한국 역시 중국발로 여겨지는 해킹 사고와 트로이목마 대량 유포 사고가 발생하는 것들이 모두 같은 맥락으로 추정하고 있다.
그러나 일본의 경우에는 이러한 중국에서 제작된 것으로 추정하는 트로이목마의 대량 유포 사고가 상당히 적은 편이다. 오히려 기존에 알려진 메일로 전파되는 넷 스카이 웜과 베이글 웜에 대한 감염 피해가 큰 것으로 분석하고 있다. 그러나 일본의 경우에는 악성코드에 직접적인 피해보다 중국으로부터 유입되는 서비스 거부 공격 등의 일련 해킹 시도에 대한 우려가 더 커지고 있는 것으로 보여지고 있다. 일본의 악성코드 동향과 유사하게 유럽 지역 역시 메일 전파되는 넷 스카이 웜과 자피 웜에 대한 감염 피해가 큰 것으로 보고 되고 있으며 이와 더불어 심비안 운영체제에서 작동하는 모바일 악성코드도 꾸준히 등장하고 있는 실정이다.

(1) 일본 악성코드 동향

작성자: 김소헌 주임연구원(sopara@ahnlab.com)

2005년 9월 일본의 보안동향과 관련한 중요 이슈 중 하나는 중국을 발신지로 하는 다량의 네트워크 트래픽이 발생한 것이다. 아래의 [그림1]은 9월 한달 일본의 네트워크 포트별 사용 통계를 나타낸 것이다. 9월 7일과 20일을 전후로 하여 여러 포트를 이용한 트래픽이 급격하게 증가한 것을 볼 수 있다.

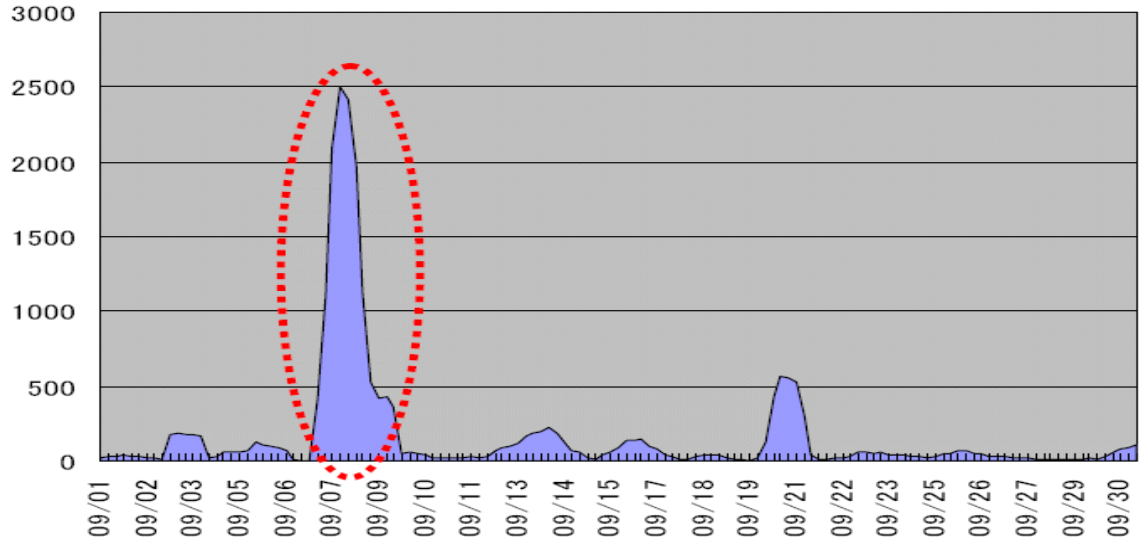


[그림1] 일본의 네트워크 포트 별 사용현황

Copyright © AhnLab Inc,. All Rights Reserved.

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

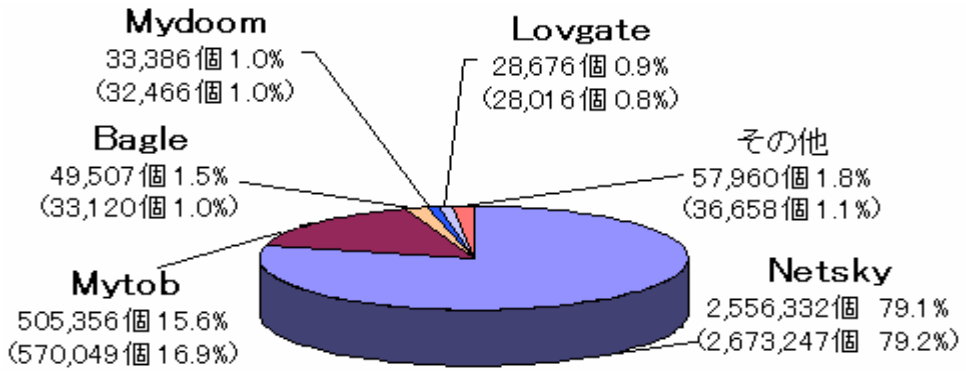
[그림2]는 일본의 IPA(www.ipa.go.jp)에서 관측한 중국을 발신지로 하는 TCP 7000번 포트의 트래픽을 나타낸 것이다. 9월 7일을 전후하여 해당 포트의 트래픽이 급격하게 늘어난 것을 알 수 있다. IPA에서는 이러한 트래픽 발생 원인을 중국 측으로부터의 서비스 거부 공격으로 파악했는데 전월을 비롯하여 최근 중국을 진원지로 한 공격이 빈번하게 발생하고 있으므로 이에 대한 주의가 필요하다.



[그림2] TCP 7000 Port 트래픽 현황

1. 일본 유행 악성코드 유형별 발생현황

2005년 9월 일본의 악성코드 동향은 전월과 크게 차이가 없다. [그림3]은 IPA에서 발표한 악성코드 통계 자료 중 일본에서 9월 탐지된 악성코드의 종류별 탐지 통계를 나타낸 것으로 넷스카이웜 (Win32.Netsky.worm)의 전파가 다른 악성코드에 비해 월등히 많은 것을 볼 수 있다. 베이글웜(Win32.Bagle.worm)의 전파가 전월에 비해 많이 늘어난 것과 통계에 나오지 않은 다른 악성코드들의 확산도가 높아진 것은 주목할만한 점이다.



[그림3] 악성코드 발견 건수 통계

Copyright © AhnLab Inc,. All Rights Reserved.

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

[표1]은 2005년 9월에 IPA에 신고된 악성코드 감염 통계를 나타낸 것이다. 전월과 동일하게 넷스카이 웜에 의한 피해 건수가 가장 많은 수를 차지하고 있으며 감염 피해 또한 증가한 것을 알 수 있다.

Window/Dos Virus	금월피해	Macro Virus	금월피해	Script Virus	금월피해
	전월피해		전월피해		전월피해
Win32/Netsky	1057	Xm/Laroux	9	VBS/Redlof	58
	999		11		72
Win32/Mytob	634	XF/Sic	5	VBS/Loveletter	9
	536		0		6
Win32/Mydoom	379	W97M/Divi	3	Wscript/	5
	352		3	Kakworm	0
Win32/Bagle	328	WM/Cap	2	VBS/Soraci	5
	303				5
Win32/Lovgate	242	X97M/Barisada	2	VBS/Freelink	4
	213		3		0
Win32/Klez	210	WM/Sarsnan	2	VBS/Gedza	2
	255		3		0

[표1] 악성코드 피해 신고 현황

2. 악성코드의 감염 경로별 통계

[표2]는 악성코드의 감염 경로 별 통계를 표로 나타낸 것으로써 메일을 통한 감염 피해가 가장 많은 부분을 차지하고 있는 것을 알 수 있다. 메일을 통한 감염 이외에도 네트워크를 통한 피해 건수가 증가하고 있는 것을 알 수 있는데 이는 IRCBot과 같은 OS의 취약점을 이용하여 자신을 복제하는 웜의 지속적인 증가가 원인으로 분석 된다.

감염경로	피해 건수					
	2005년 9월		2005년 8월		2004년 9월	
메일	4,524	95.8%	4,290	98.7%	5,291	97.9%
외부의 모체	0	0%	4	0.1%	4	0.1%
다운로드	0	0%	1	0.1%	13	0.2%
네트워크	187	4.0%	171	0.9%	93	1.7%
기타	12	0.3%	4	0.2%	3	0.1%

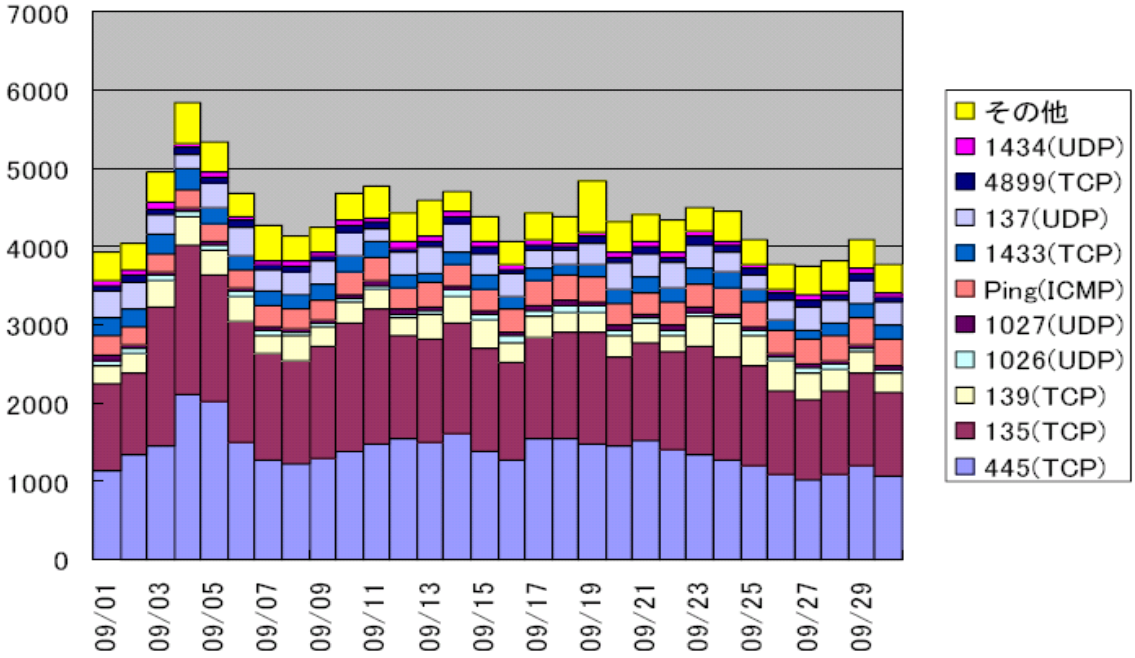
[표2] 악성코드 감염 경로 통계

Copyright © AhnLab Inc,. All Rights Reserved.

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

3. 일본 네트워크 트래픽 현황

일본에서 발생한 네트워크 트래픽 통계에서 가장 많이 사용되는 포트는 TCP 135번 포트와 TCP 445번 포트이다. 해당 포트들은 윈도우 운영체제에서 인증과 관련하여 사용되지만 웜과 같은 악성코드들에서 시스템의 취약점을 이용하여 시스템 권한을 획득하기 위해 사용되므로 주의가 필요하다. 아래의 [그림4]는 네트워크 사용 포트의 발신지별 통계를 나타낸 것이다. 위의 [그림1]과 비교하여 보았을 때 9월 7일 발생한 TCP 7000번 포트의 트래픽 증가와 관련하여 발신지의 양이 많지 않은 것을 알 수 있는데 이는 특정 IP에서 다량의 트래픽이 발생했을 가능성이 높음을 짐작할 수 있게 해준다.



[그림4]발신지 별 네트워크 포트 사용현황

(2) 중국 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

9월 중국 악성코드 동향은 전반적으로 트로이목마가 강세를 보이고 있는 가운데 Backdoor.Gpigeon (V3 진단명 Win-Trojan/GrayBird)에 의한 감염 신고가 증가하고 있는 상황을 보이고 있다. 8월까지 급격한 증가세를 보이던 Trojan.PSW.LMir(V3 진단명 Win-Trojan/LmirHack)는 9월에 이르러서 잠시 감소하는 추세를 보이고 있으나 아직까지 많은 감염 피해를 유발하고 있는 것으로 추정된다. 그리고 악성 IRCBot 웜(V3 진단명 Win32/IRCBot.worm)은 취약점을 이용해 감염되는 기법으로 인해 전반적으로 지난 달과 유사

Copyright © AhnLab Inc,. All Rights Reserved.

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

하게 현상 유지를 하고 있는 것으로 분석된다. 이러한 특징을 바탕으로 9월 악성코드의 동향은 어떠한 변화가 있었는지 살펴보도록 하자.

1. 악성코드 TOP 5

순위 변화	순위	Rising
↑ 1	1	Backdoor.Gpigeon
↓ 1	2	Trojan.PSW.LMir
-	3	Backdoor.Rbot
New	4	Trojan.PSW.QQRobber
New	5	Backdoor.Sdbot

[표1] 2005년 9월 Rising 악성코드 TOP 5

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

순위 변화	순위	JiangMin
↑ 1	1	Backdoor/SdBot.atp.Rootkit
↓ 1	2	Trojan/Script.Seeker
New	3	Exploit.MhtRedir
↓ 1	4	Trojan/QQMsg.Zigui.b
↓ 1	5	Trojan/WebImport

[표2] 2005년 9월 JiangMin 악성코드 TOP 5

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

[표 1]과 [표 2]는 중국 로컬 백신 업체인 라이징(Rising)과 강민(JiangMin)의 9월 악성코드 TOP 5이다. 먼저 라이징의 순위를 살펴본다면 한국과 유사하게 트로이목마 류의 악성코드의 대거 확산과 그에 따른 다양한 피해사례가 발생하고 있는 것을 알 수 있다. 특히 지난 8월 1위로 급상승한 Trojan.PSW.LMir (V3 진단명 Win-Trojan/LmirHack)은 9월 달에 이르러서는 2위로 감소 추세를 보였다. 특히 엘미르핵 트로이목마는 국내에서 개발되어 중국 등 외국으로 수출되는 잘 알려진 몇몇 온라인게임과 국내에서 많은 회원을 확보하고 있는 온라인 게임 웹 사이트들의 사용자 계정과 암호를 유출하기 위해 제작되었다. 특히 해당 온라인 게임들은 게임 내에서 사용하는 사이버머니가 오프라인에서 현금으로도 유통되고 있다는 점으로 미루어 이를 노리고 유포되고 있는 것으로 추정하고 있다. 엘미르핵 트로이목마를 제치고 1위를 차지한 Backdoor.Gpigeon(V3 진단명 Win-Trojan/GrayBird)는 한국의 국내 고객들에게도 비교적 많은 샘플 접수가 있었던 만큼 중국 내에서도 이와 비슷하게 많은 감염 피해가 있었던 것으로 분석된다. 그레이버드 트로이목마는 그 감염기법이 정상적인 인터넷 익

Copyright © AhnLab Inc,. All Rights Reserved.

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

스플로러를 백 그라운드 프로세스로 실행한 후 트로이목마 자신을 해당 프로세스의 핸들로 삽입되는 기법을 사용하여 프로세스를 확인하는 것만으로는 쉽게 감염 여부를 확인하기가 어렵다. 게다가 외부로 통신을 시도할 경우에는 정상적인 TCP 80번 포트를 사용하여 리버스 커넥션을 시도함으로 방화벽과 침입탐지 시스템들을 회피하는 기법도 동반하고 있어 감염에 따른 피해가 클 것으로 우려된다. 그리고 중국에서 개발한 QQ 메신저를 이용한 트로이목마의 변형 중 하나인 Trojan.PSW.QQRobber(V3 진단명 Win-Trojan/QQRob)이 4위를 차지하고 있다. QQ 롭 트로이목마는 중국 내에서 가장 많은 사용자를 확보하고 있는 QQ 메신저를 이용하여 전파되며 감염된 시스템의 사용자 정보 등을 특정 메일 주소로 전파하는 기능을 가지고 있다. 그러나 중국 내에서만 사용하는 QQ 메신저의 지역성으로 인해 한국이나 기타 국가에서는 QQ 롭 트로이목마는 접수되고 있지 않다.

다음은 강민의 TOP 5을 살펴보도록 하자. 지난 8월 1위를 차지하고 있던 Trojan/Script.Seeker은 은폐기능을 수행하는 루트킷을 포함하고 있는 악성 IRCBot 웜(V3 진단명 Win32/IRCBot.worm)에게 1위 자리를 내주고 2위로 물러나게 되었다. 라이징 순위와 비교해본다면 중국 내에서 악성 IRCBot 웜은 취약점이 존재하는 운영체제를 대상을 공격하는 기법으로 인해 네트워크 상에서 악성 IRCBot 웜의 패킷이 많이 발생하고 있는 것으로 추정된다. 그리고 중국 내 운영체제가 가지고 있는 취약점을 제거하는 패치를 설치하지 않은 시스템이 많이 존재하고 있는 것으로도 추정할 수 있을 것이다. Exploit.MhtRedir(V3 진단명 HTML/MhtRedir)은 최근 몇 개월 사이 트로이목마의 대량 확산의 주된 원인으로 꼽히는 스크립트 파일이다. 그레이버드 트로이목마와 엘미르 핵 트로이목마의 확산 경로를 추적해 보면 대부분이 보안이 취약한 웹 서버를 해킹한 후 해당 웹 페이지 중간에 iFrame 태그를 삽입하여 제 3의 시스템에서 트로이목마를 다운로드 하도록 유도하고 있다. 그 중에서 HTML/MhtRedir은 운영체제에 취약점을 가지고 있는 시스템에서 다운로드 한 트로이목마를 실행하는 데 사용되고 있다. 이로 인해 단 기간에 많은 시스템들이 앞서 언급한 트로이목마들에 대한 감염이 가능하였던 것으로 분석하고 있다.

2. 주간 악성코드 순위

순위	1 주	2 주	3 주	4 주
1	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon
2	Trojan.PSW.QQRobber	Backdoor.Rbot	Trojan.PSW.LMir	Worm.Mail.Bagle
3	Trojan.PSW.LMir	Trojan.PSW.LMir	Backdoor.Rbot	Worm.Linux.Ramen
4	Backdoor.Rbot	Backdoor.Sdbot	Trojan.PSW.QQRobber	Backdoor.Rbot
5	Backdoor.Sdbot	Trojan.PSW.QQpass	Backdoor.Sdbot	Trojan.PSW.LMir

[표3] 2005년 9월 Rising 주간 악성코드 순위

Copyright © AhnLab Inc,. All Rights Reserved.

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

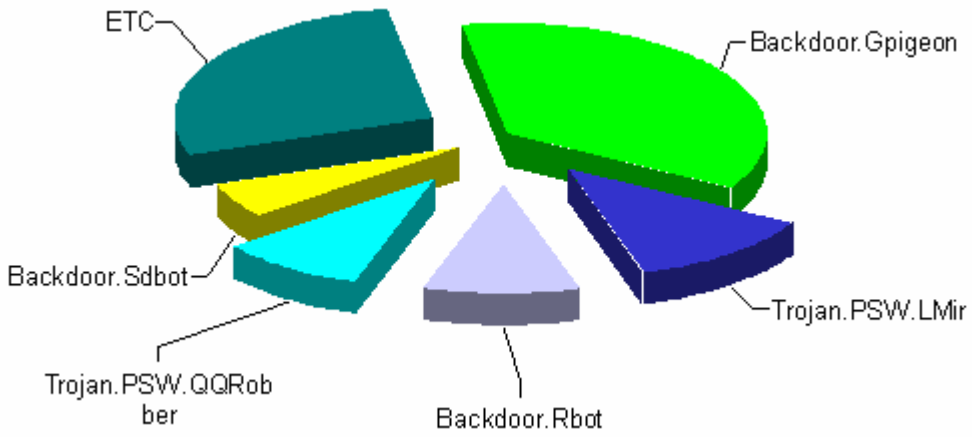
순위	1 주	2 주	3 주	4 주
1	Backdoor/SdBot.atp.Rootkit	Backdoor/SdBot.atp.Rootkit	Backdoor/SdBot.atp.Rootkit	Backdoor/SdBot.atp.Rootkit
2	Trojan/Script.Seeker	Trojan/Script.Seeker	Exploit.MhtRedir	Trojan/Script.Seeker
3	Trojan/QQMsg.Zigui.b	Trojan/QQMsg.Zigui.b	Trojan/Script.Seeker	Exploit.MhtRedir
4	Exploit.MhtRedir	Exploit.MhtRedir	Trojan/QQMsg.Zigui.b	Trojan/WebImport
5	Trojan/WebImport	Trojan/WebImport	Backdoor/Rootkit.Agent.b	Trojan/QQMsg.Zigui.b

[표4] 2005년 9월 JiangMin 주간 악성코드 순위

[표3]과 [표4]는 라이징과 강민의 주간 악성코드 순위 도표이다. 먼저 라이징의 순위를 본다면 4주 연속으로 그레이버드 트로이목마가 1위를 차지하고 있는 것으로 분석된다. 그리고 QQ 롭 트로이목마는 1주차에서는 2위로 등장하였으나 4주차에서는 순위에 포함되어 있지 않은 것으로 미루어 9월 1주차에서 일시적인 확산을 보였었으나 그 확산이 감소 추세를 보였던 것으로 분석된다.

다음으로 강만의 주간 악성코드 순위를 본다면 라이징과 유사하게 은폐기능을 수행하는 악성 IRCBot 웜이 4주간 1위를 차지하고 있었다. HTML/MhtRedir 은 급격한 순위 변동은 없었던 것으로 보이며 지속적으로 발견이 되고 있는 것으로 분석된다.

3. 악성코드 분포



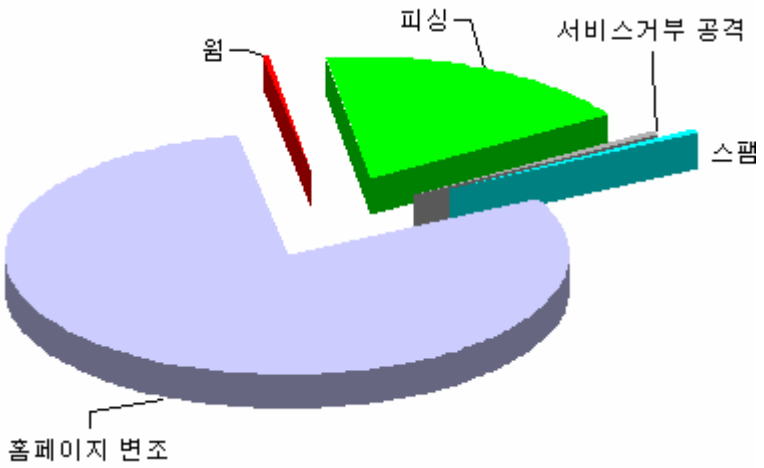
[그림 1] 2005년 9월 Rising의 악성코드 분포

Copyright © AhnLab Inc,. All Rights Reserved.

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

9월 악성코드 분포에서는 그레이버드가 36%로 가장 큰 비중으로 차지하고 있다. 그러나 순위에 포함되지 않은 기타 악성코드들이 그레이버드에 이어 전체의 27.7%를 차지하고 있어 기타 악성코드들의 형태가 트로이목마를 중심으로 다양화 되고 있는 것으로 추정된다. 그러나 전반적인 악성코드 감염 피해 신고 건수가 8월 547건에서 9월 1347건으로 3배 가까운 수치가 증가한 것을 감안한다면 엘미르핵 트로이목마와 그레이버드 트로이목마의 분포는 지난 달과 비교하여 크게 증가한 것으로 생각해 볼 수 있다.

4. 보안 사고 통계



[그림 2] 2005년 9월 CNCERT/CC의 보안사고 분포

9월 중국 CNCERT/CC의 보안 사고 분포는 8월과 비교하여 전반적인 수치가 크게 감소한 것으로 분석되며 트로이목마와 해킹 사고는 9월에는 발생하지 않은 것으로 집계되었다. 그리고 9월의 가장 큰 변화는 8월 1042건으로 가장 큰 증가치를 보였던 홈페이지 변조가 9월에 이르러서는 절반 정도 수준인 511건으로 크게 감소하였다. 그러나 피싱 관련 사고는 8월 66건으로 집계되었으나 9월에는 122건으로 유일하게 증가한 것으로 분석되었다.

(3) 세계 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2005년 9월 악성코드는 8월과 큰 변화가 없는 상태이다. 소포스[1]와 카스퍼스키랩[2]에 따르면 여전히 넷스카이 변형이나 자피 변형이 1위를 차지하고 있으며 마이톱 변형들이 순위에 들어있다. 마이톱 제작 용의자가 검거되었지만 그가 배포한 웜 소스는 여전히 여러 변형을 양산해 내고 있다.

[1] http://www.sophos.com/pressoffice/pressrel/uk/toptensep05.html
[2] http://www.viruslist.com/en/analysis?pubid=171283978

Copyright © AhnLab Inc,. All Rights Reserved.

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

9월에는 베이글 변형이 20 개 이상 발견되었지만 예전처럼 널리 퍼지지 않았다. 베이글 제작자는 웜의 확산보다 베일글 변형을 통해 스팸 메일을 보내 얻는 금전적 이득에 더 치중하는 것으로 보인다.

심비안OS 악성코드가 계속 등장하고 발전하고 있는데 Cardtrap 로 알려진 트로이목마는 휴대폰에 설치된 메모리카드에 윈도우 웜을 몰래 복사해 두는 것으로 알려졌다. 메모리카드를 사용자 컴퓨터의 카드리더기에 꽂으면 웜이 자동 실행될 수 있다.

모질라 공식사이트에 업로드된 한국어 버전의 리눅스 모질라와 썬더버드에 리눅스 바이러스인 Linux/RST 바이러스가 발견되었다. 이 바이러스는 2004년 한국에서도 발견된 바이러스로 리눅스 바이러스도 여전히 존재함을 알 수 있다.

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 - 악성코드 재실행 기법

작성자: 양하영 연구원(hyyang@ahnlab.com)

최근에 악성코드뿐만 아니라 스파이웨어에서도 실행과 동시에 자신의 동작상태를 감시하여 비정상적인 종료가 발생할 경우 재실행하는 기능을 가지고 있는 샘플이 발견되고 있다. 이러한 기능은 악성코드가 자신을 보호하기 위해 사용하는 방법으로 현재 다양한 기법들이 사용되고 있다. 만약, 이러한 증상을 나타내는 악성코드에 감염될 경우, 사용자는 해당 악성 프로세스를 수동으로 삭제할 수 없으므로 적절한 대응을 할 수 없게 된다.

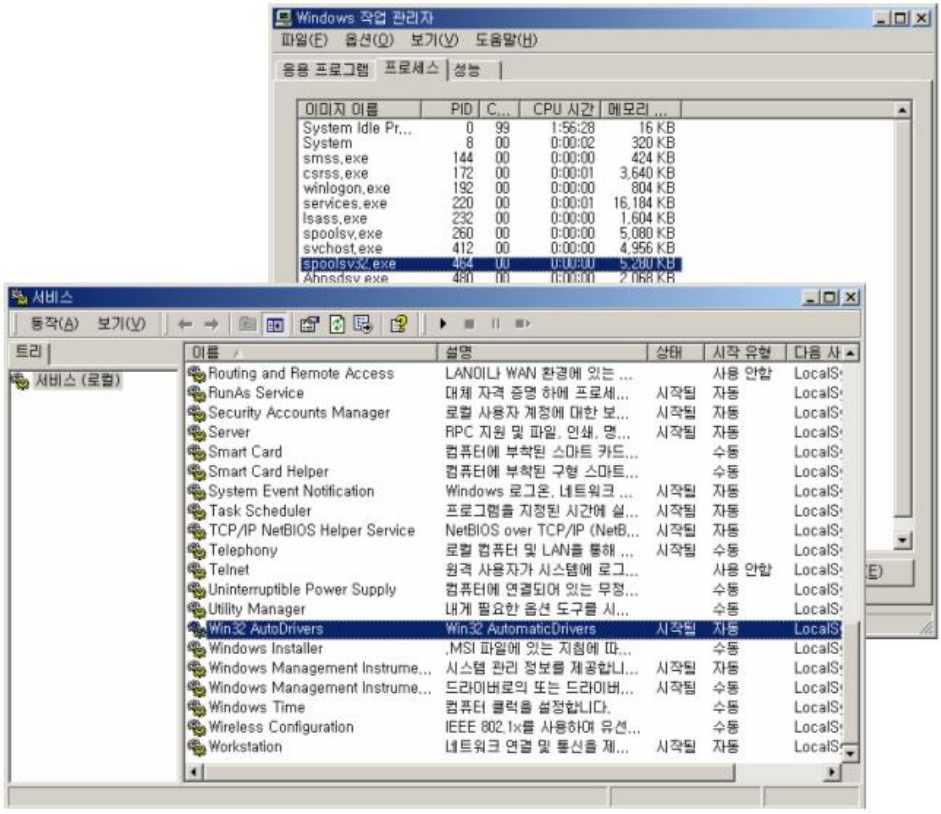
현재까지 이러한 종류의 악성코드가 빈번하게 발생하고 있지는 않지만, 웜(worm)과 같이 전파력이 높은 악성코드에서 이러한 기법이 사용될 경우, 사용자에게 큰 피해를 줄 수 있을 것으로 예상된다. 따라서, 본 컬럼에서는 현재까지 접수된 샘플 중 이러한 증상을 나타내는 악성코드들을 유형별로 분류하여 각각의 증상들을 살펴보고 나아가 적절한 대처방법을 제시하고자 한다.

1. 서비스 재시작을 통한 실행

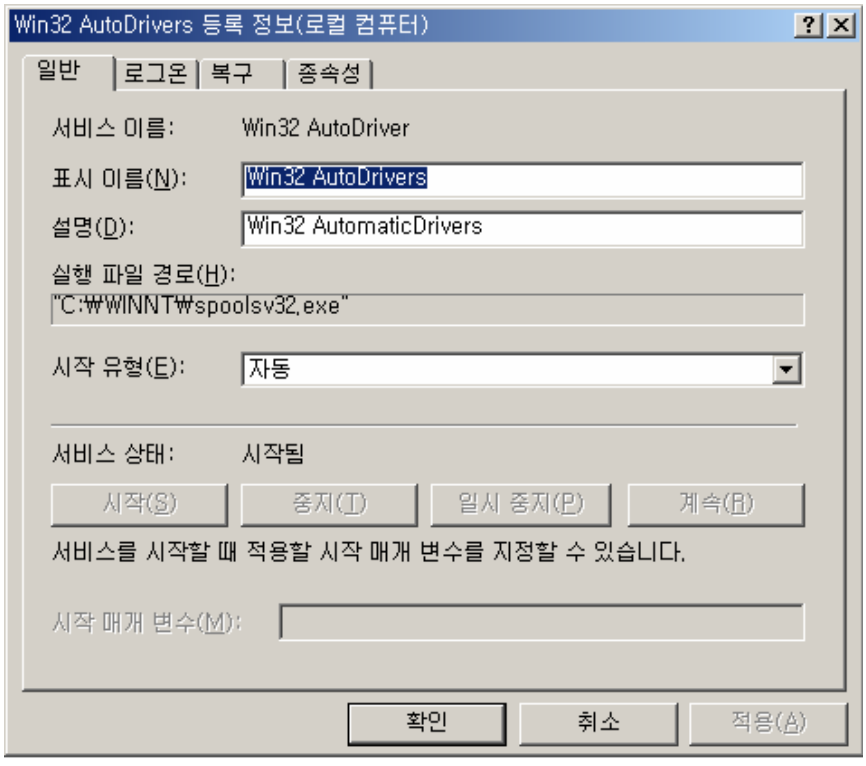
해당 악성코드가 실행되면 사용자 시스템에 서비스로 자동 실행되도록 하며, 프로세스 강제 종료를 통해 해당 서비스가 종료될 경우 자동으로 재시작하도록 서비스를 설정한다. 예를 들어, Win32/IRCBot.worm.48600로 진단하는 악성코드가 실행될 경우, [그림 1]과 같이 사용자 컴퓨터의 윈도우 폴더에 "spoolsv32.exe"라는 파일을 생성하며, 동시에 "Win32 AutoDrivers" 라는 이름의 서비스가 자동 실행된다. 윈도우 시스템에서 정상적으로 동작하는 일반적인 서비스들과는 달리 "Win32 AutoDrivers"의 경우, [그림 2]와 같이 사용자가 수동으로 서비스를 중단할 수 없도록 특정 버튼을 비활성화 상태로 변경한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림 1] 프로세스 생성 및 서비스 등록화면

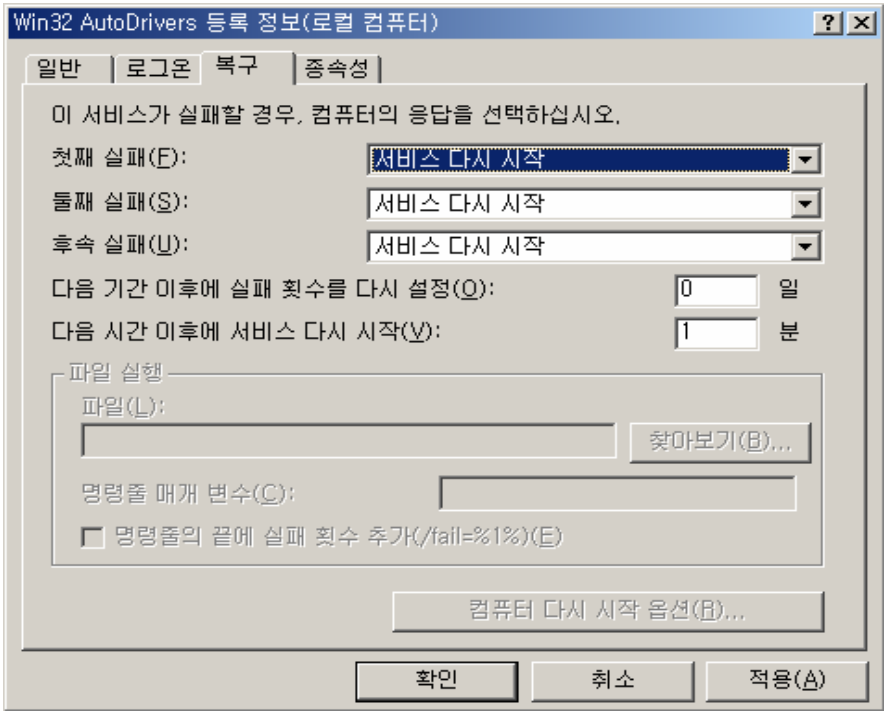


[그림 2] "Win32 AutoDrivers"의 등록정보

Copyright © AhnLab Inc,. All Rights Reserved.

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

또한, 사용자가 "spoolsv32.exe" 프로세스를 강제로 종료할 경우(서비스 실패가 발생할 경우), 해당 서비스를 자동으로 다시 시작하도록 [그림 3]와 같이 설정되어 있다. (일반적으로 정상적인 서비스의 경우, 서비스 실패 시 컴퓨터의 응답상태는 "서비스 다시 시작"이 아닌 "동작하지 않음"으로 설정되어 있다.) 따라서, 사용자는 해당 프로세스를 종료할 수 없으며 나아가 윈도우 폴더에 위치한 "spoolsv32.exe" 파일을 삭제할 수 없다. 이와 같은 악의적인 서비스 자동실행 및 복구설정의 변경은 악성코드에 의해 사용자 컴퓨터의 특정 레지스트리 값이 설정됨으로 인해 발생한다.



[그림 3] 서비스 실패에 대한 컴퓨터 응답

해당 악성코드에 대한 대처방법으로 첫 번째 방법은 "Win32 AutoDrivers" 라는 서비스의 등록정보에서 복구항목의 내용 중 서비스가 실패할 경우 컴퓨터의 응답을 "서비스 다시 시작"이 아닌 "동작하지 않음"으로 변경한 후, (아래의 링크에서 제시한 수동조치방법을 참고) 'Process Explorer'라는 도구를 이용해서 해당 프로세스를 강제 종료시킨 후 윈도우 폴더에 위치한 "spoolsv32.exe" 파일을 삭제한다.
수동조치방법: http://info.ahnlab.com/securityinfo/info_view.jsp?seq=5826&category=01

다른 방법으로는, "Win32 AutoDrivers" 라는 서비스의 등록정보에서 일반항목의 내용 중 시작유형을 "자동"에서 "수동" 혹은 "사용 안함"으로 설정한 후 위와 동일한 강제종료 및 파일삭제 작업을 수행한다.

마지막 방법으로 'Process Explorer'라는 도구를 사용할 수 없는 경우, 사용자 컴퓨터를 안전모드로 재부팅 한 후 윈도우 폴더에 위치한 "spoolsv32.exe" 파일을 삭제함으로써 해당

Copyright © AhnLab Inc,. All Rights Reserved.

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

프로세스의 재실행을 차단할 수 있다.

2. 반복적인 프로세스 생성 및 종료작업을 통한 재실행

해당 악성코드가 실행되면, 빠른 시간 동안 프로세스의 생성과 종료작업을 계속 반복수행함으로써 사용자가 수동으로 해당 프로세스를 종료할 수 없도록 한다.

이러한 증상을 나타내는 악성코드는 자신이 생성한 프로세스를 짧은 시간 동안 생성과 소멸을 반복적으로 수행 함으로써 사용자가 수동으로 해당 프로세스를 삭제하지 못하도록 한다. 즉, 사용자가 수동으로 악성 프로세스를 종료하려고 하는 순간 이미 해당 프로세스는 종료되어 존재하지 않으며, 또 다른 동일 프로세스가 생성되어 있다. 악성코드 자신이 생성 및 소멸 작업을 계속적으로 반복함으로써 사용자는 해당 프로세스를 삭제할 수 없다. 이러한 유형의 악성코드의 경우, 사용자가 수동으로 해당 프로세스를 삭제할 수 있는 방법은 없으며, 안티 바이러스 혹은 안티 스파이웨어 제품을 사용하여 치료해야 한다.

3. 자식 프로세스 생성을 통한 재실행

해당 악성코드가 실행되면, 동시에 자신과 동일한 자식 프로세스를 추가 생성하며 사용자가 이 두 개의 프로세스 중 하나의 프로세스를 강제 종료할 경우, 다른 하나가 이를 감지하여 종료된 프로세스를 재실행하도록 한다.

이러한 증상을 나타내는 악성코드는 실행과 동시에 자신과 동일한 자식 프로세스를 생성한다. 두 개의 동일 프로세스는 서로를 감시하는 작업을 수행하며 이를 통해 하나의 프로세스가 종료될 경우, 다른 프로세스가 자신과 동일한 새로운 프로세스를 재실행 시킨다. 이러한 기법은 사용자가 동시에 두 개의 프로세스를 종료할 수 없다는 점을 이용한 것이다. 이와 유사한 방법으로 실행 시 자신과 동일한 프로세스를 무수히 많이 생성함으로써 사용자가 해당 프로세스의 종료를 어렵게 하는 경우도 있다. 이러한 경우는, 사용자에게 단순히 해당 악성코드를 삭제하는 작업을 어렵게 할 뿐만 아니라 시스템에도 큰 부하를 주어 다른 작업을 원활하게 수행할 수 없도록 한다. 이러한 유형의 악성코드에 대처하는 방법은 두 번째 유형과 같이 사용자에 의해 수동으로 삭제할 수 있는 방법은 없으며, 안티 바이러스 혹은 안티 스파이웨어 제품을 사용하여 치료해야 한다.

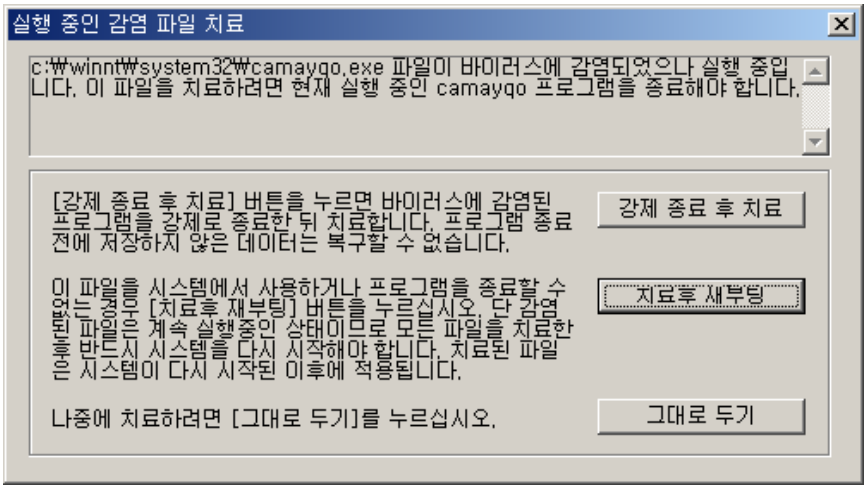
4. 악성코드 삽입을 통한 재실행

해당 악성코드가 실행되면, 사용자 시스템의 특정 정상 프로세스에 악성코드를 삽입하고 이를 통해 자신이 종료될 경우를 감지하여 재실행 하도록 한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

예를 들어, Win-Trojan/Agent.83456.K의 경우, 해당 악성코드는 사용자 컴퓨터에서 정상적으로 동작하고 있는 프로세스인 "EXPLORER.EXE"와 "WINLOGON.EXE"에 악의적인 코드를 삽입한다. 이러한 유형의 악성 코드가 수행하는 일은 악성 프로세스의 동작을 감시하여 해당 프로세스가 비정상적으로 종료될 경우 이를 다시 실행시키게 하는 등의 작업을 수행한다. 또한, 해당 프로세스가 종료된 후 재 시작할 때마다 매번 프로세스 이름을 랜덤하게 생성하여 실행함으로써 사용자로 하여금 삭제를 더욱 어렵게 한다. 이러한 유형의 악성코드의 경우, 해당 프로세스를 완전히 종료시키기 위해서는 정상 프로세스인 "EXPLORER.EXE"를 종료하여야 한다. V3 제품에서 이 악성코드를 치료하기 위해서는 [그림 4]와 같이 치료옵션에서 "치료후 재부팅"을 선택해야 한다. "강제 종료 후 치료"를 선택할 경우, 치료가 정상적으로 이루어지지 않으며, 해당 버튼이 비활성화 된다. 따라서, 사용자는 처음부터 "치료후 재부팅"을 선택하여 정상적인 파일 삭제가 이루어지도록 해야 한다.



[그림 4] V3에서의 치료옵션

지금까지 최근에 발생한 악성코드들 중에서 자신을 삭제할 수 없도록 방어기법을 사용하는 샘플들을 몇 가지 유형별로 나누어 살펴보았다. 향후에는 이러한 유형들 이외에도 보다 복잡한 기법을 사용하여 악성코드 자신을 삭제할 수 없도록 방어하는 샘플들이 증가할 것으로 예상된다. 또한, 이러한 기법 중의 일부는 사용자뿐만 아니라 안티 바이러스 제품에서 완전한 치료가 어렵게 할 수도 있을 것이다. 실제로 자신이 종료될 경우를 감시하여 재시작 하지는 않지만, 사용자에게 악성코드 자신을 볼 수 없도록 숨김(Stealth) 기능을 사용하는 경우도 있다. 이와 같이 다양한 자기 방어기능을 갖고 있는 악성코드에 효과적인 대응을 하기 위해서 안티 바이러스 및 안티 스파이웨어 제품들도 이러한 기법들에 대해서 보다 세심한 분석작업이 이루어져야 하며, 체계적으로 그 유형들을 파악하고 대처하는 작업이 필요하다. 나아가 앞에서 살펴본 유형들 중 마지막 경우에서처럼 정상적으로 동작하고 있는 프로세스인 "EXPLORER.EXE"를 종료해야 할 경우, 사용자 시스템을 재시작하지 않고도 효과적으로 대응 할 수 있도록 하는 등의 개선작업이 이루어져야 한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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