ASEC Report 3월

® ASEC Report

2005. 04

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

트로이목마와 유해가능 프로그램의 피해 증가…

3월은 2월에 비해 악성코드 피해 및 신종(변형) 발견 건수가 감소하는 현상을 보였다. 이 수치는 2005년 들어 계속 하락하는 추세를 보이고 있다. 3월 악성코드 피해는 작년부터 계속 부동의 1위를 차지하고 있는 넷스카이.29568 웜의 피해가 다소 감소하면서 전반적인 피해건수가 감소하는 추세를 보였다. 그러나 3월의 피해신고된 악성코드 현황을 보면 웜에 의한 피해는 감소한 반면, 트로이목마에 의한 피해는 15%나 증가한 수치를 나타내고 있다. 이러한 추세는 신종(변형) 발견에서도 동일한 현상을 보이고 있다. 기존에 많이 발견되던 악성 아이알씨봇 변형 발견은 지속적인 감소추세를 보이는 반면, 트로이목마와 유해가능 프로그램이 배로 증가한 수치를 보이고 있다. 트로이목마가 스파이웨어나 악성코드들과 연동되는 양상을 보이면서 작년 하반기부터 증가하는 추세를 보이고 있는 것이다. 3월에는 마이탑 웜 변형의 발견이 많았는데, 2월말부터 4월초에 이르기까지 총 18종의 변형이 발견 보고되어 주목을 받았다. 3월에는 한글키워드 서비스에 대한 업체간의 경쟁이 심해지면서 한글 키워드 플러그인을 설치하는 스파이웨어까지 등장하여 사용자의 많은 피해가 보고되었다. 이는 스파이웨어 아이가드로, 특정 키워드 및 특정 사이트 접속시에 인스톨 쉴드로 된 설치파일을 다운로드한 후 키워드 인터넷 한글 접속 도우미를 설치한다. 한국을 포함한 3월 전세계의 악성코드 피해는 매스메일러에 의한 피해가 가장 많은 것으로 나타났다. 그러나 지역적으로는 다소 차이가 있는데, 일본과 한국은 넷스카이 웜으로 인한 피해가, 중국은 백쯔 웜에 의한 피해가, 유럽지역은 자피 웜과 마이둠 웜에 의한 피해가 많은 것으로 나타났다. 이 추세는 지난 2월과 비슷한 현상으로 보이고 있는 것으로, 당분간 이 추세는 지속될 것으로 보인다. 3월에 크게 이슈가 된 시큐리티 사고나 취약점은 없었다. 다만 올해 초부터 국내 웹 해킹 대량 변조사건이 지속적으로 발견되고 있어, 이에 대한 문제점과 해결책에 대해 살펴보았다. 이달의 ASEC 컬럼에서는 신종 인터넷사기수법으로 이슈가 되었던 파밍에 대해 알아보고 그것이 향후 미칠 영향에 대해 예측해 보았다.

I. 3월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자 : 박철민 연구원(cmpark@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	462	28.0%
2	↑2	Win32/Netsky.worm.17920	61	3.7%
3	↑4	Win32/Netsky.worm.25352	54	3.3%
4	New	Win32/Netsky.worm.17424	52	3.1%
5	↑1	Win32/Netsky.worm.22016	50	3.0%
6	↑4	Win32/Netsky.worm.28008	45	2.7%
7	↓3	Win32/Sasser.worm.15872	35	2.1%
8	New	Win32/Netsky.worm.18944.B	32	1.9%
9	New	Win32/AgoBot.worm.gen	28	1.7%
10	New	Win32/LovGate.worm.128000	28	1.7%
		기타	804	48.7%
합계			1,651	100%

[표1] 2005년 3월 악성코드 피해 Top 10

2005년 3월 악성코드 피해 건수는 2005년 2월에 비해 소폭 감소한 1,651건이다. 지난 2월에 비해 다소 감소한 이유는 1위를 차지하고 있는 넷스카이.29568(Win32/Netsky.worm.29568)의 피해감소로 인해 전반적인 감염 피해수치가 낮아진 것으로 보인다. 하지만 여전히 넷스카이.29568 웜이 작년에 이어 올해도 가장 많은 보고 및 신고건수를 차지하고 있다.

작년에 이어 올해도 1위를 차지한 넷스카이.29568 웜의 특징은 다음과 같다.

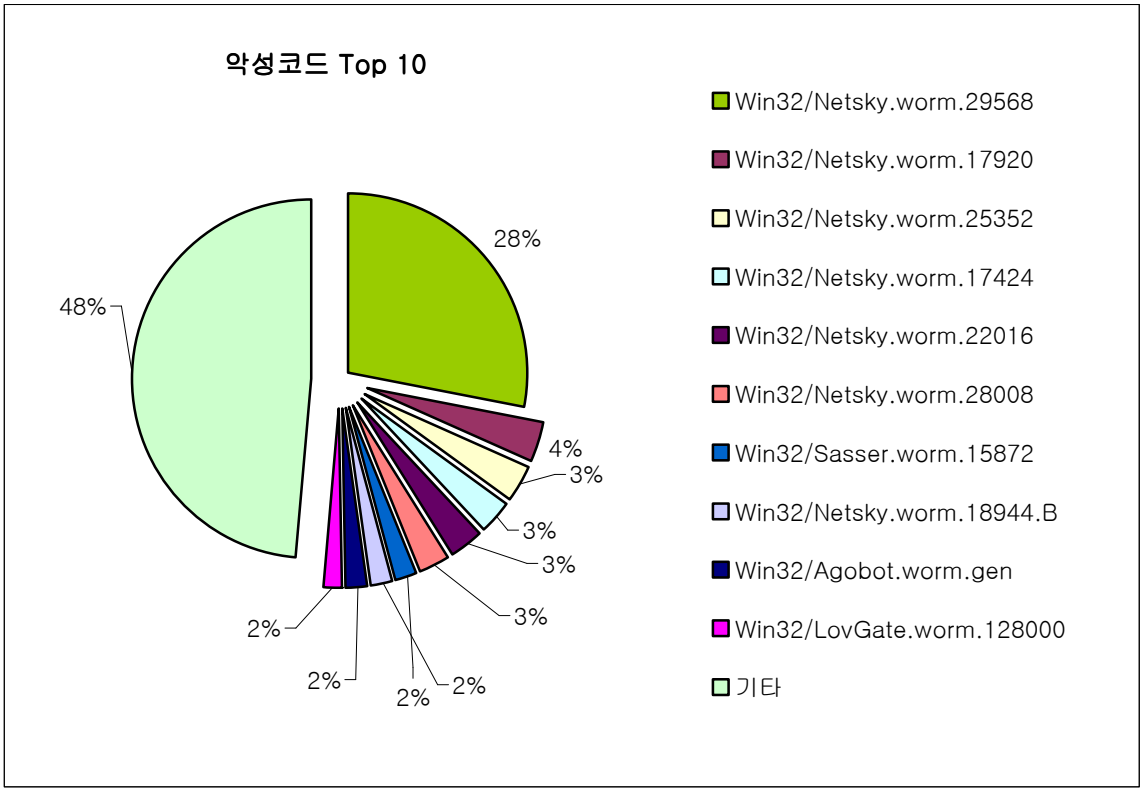
- 메일 및 공유폴더로 전파
- 메일로 전파 시 취약점 사용
- 다양한 확장자에서 메일주소 수집
- 다양한 첨부파일명과 메일 제목, 본문 등을 가지고 있음
- 특정 악성코드의 실행을 중지

작년 3월 중순경에 처음 발견된 이 웜은 초기에 상당히 많은 시스템을 감염시켜, 대량의 메일을 발송하여 전파되었으며, 아직도 감염된 시스템들이 상당수 있는 것으로 보인다.

또한 넷스카이.29568 웜의 동일한 제작자가 윈도우 취약점(MS04-011)[1]을 이용하여 시스템을 감염시키는 새서 웜(Win32/Sasser.worm.15872)도 유포시켰는데, 이 새서 웜은 작년 말에 Top 10 순위 권 밖으로 벗어났으나, 올해 1월부터 다시 등장하여 순위 권에 계속 머물고 있다.

올해 들어 다시 새서 웜 피해가 보고되는 원인으로는 공공기관, 학교 등의 새 PC 교체주기에 따른 신규시스템, OS를 재 설치한 시스템, 예전부터 취약점에 노출된 시스템 등에 의한 것으로 추정된다. 따라서, 시스템을 교체하거나 운영체제를 새로 설치할 경우에는 취약점을 이용한 웜의 감염을 막기 위해 가장 먼저 관련 전용백신이나 백신제품을 설치한 후, 해당 운영체제의 모든 취약점에 대한 보안패치를 신속히 적용해 주는 것이 중요하다.

3월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.

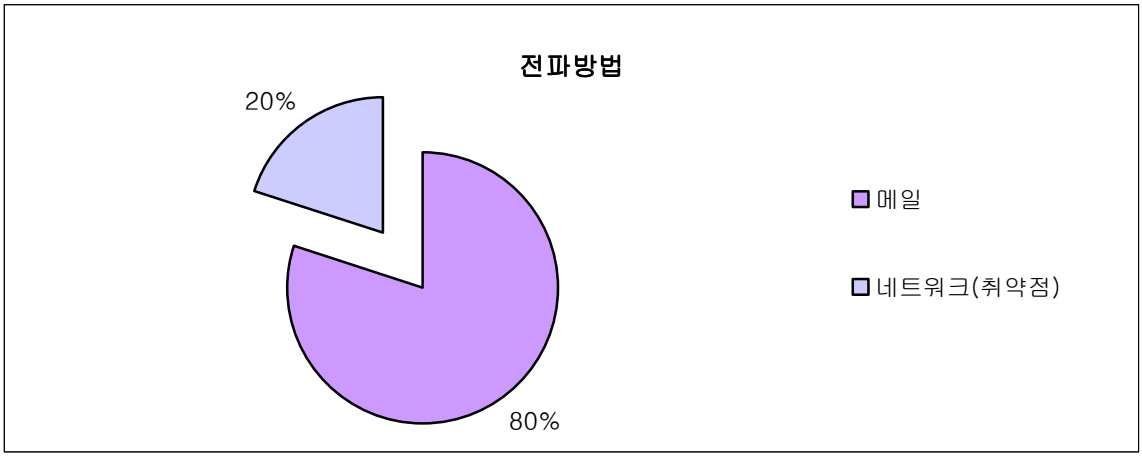


[그림1] 2005년 3월 악성코드 피해 Top 10

3월 악성코드 Top 10 전파방법별 현황

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

[1] http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx



[그림2] 악성코드 Top 10의 전파방법별 현황

앞서 언급한 것과 같이 악성코드가 이용하는 전파방법의 대다수가 이메일을 이용하였으며, 이는 지난달과 동일한 현황으로써 매스메일러(Mass Mailer)에 의한 피해가 대부분을 차지하고 있음을 보여주고 있다. 또한 네트워크(취약점)을 통해 전파되는 유형도 꾸준히 나타나고 있기 때문에 사용자들은 시스템의 취약점들을 주기적으로 패치하여 재감염의 피해가 발생하지 않도록 주의하여야 한다.

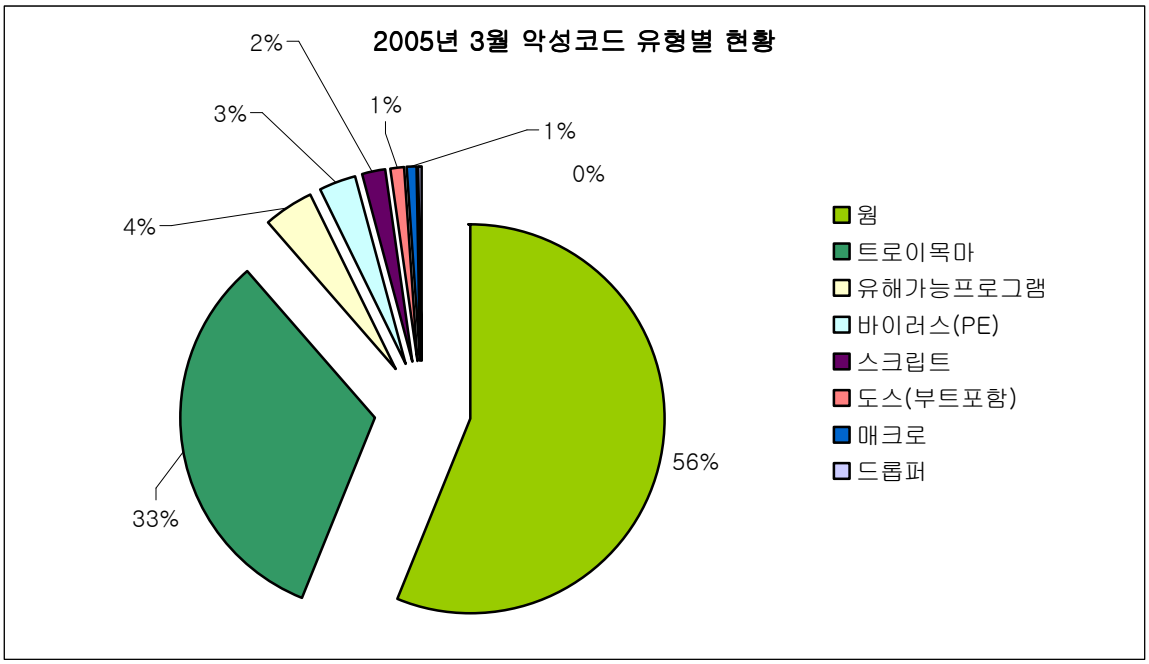
월별 피해신고 악성코드 건수 현황

3월에 피해 신고된 악성코드는 490개이다. 지난 2월에 비해 소폭 감소하였으며, 1월부터 지속적으로 감소하고 있다는 것을 알 수 있다. 이것은 V3 엔진의 악성 아이알씨봇(IRCBot) 진단기능이 향상된 결과로 볼 수 있다.

[그림3] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림4]와 같다.



[그림4] 악성코드 유형별 현황

다양한 종류와 많은 변형을 가진 웜이 2월에 비해 18%나 감소하였다. 반면 트로이목마는 2월에 비해 15%나 증가하였다. 이것은 일부 트로이목마(Agent, Downloader, StartPage, Ranky, Small)의 증가가 주요원인으로 보인다.

악성코드 피해건수에 비해 신고된 악성코드 수는 지난 2월에 이어 3월에도 눈에 띄게 감소하였다. 이것은 V3 엔진의 강화에 따른 결과로 보인다. 하지만 여전히 메일을 통해 전파되는 악성코드의 피해건수가 줄어들지 않고 있는 점과 윈도우 취약점을 이용하여 전파되는 악성코드가 계속 발견되고 있다는 점에서 사용자들은 의심스러운 메일은 열어보지 말고 바로 삭제하고, 신규 취약점이 발견될 경우 즉시 윈도우 업데이트 사이트에 접속하여 보안 패치를 적용하여야 한다. 또한 웹으로 유포되는 스파이웨어를 대비하여 의심되는 웹사이트에는 접근하지 않고, 윈도우 XP일 경우 SP2로 업그레이드하여 불필요한 ActiveX는 다운로드 받지 않도록 예방하여야 된다.

(2) 신종(변형) 악성코드 발견 동향

작성자 : 정진성 주임연구원 (jsjung@ahnlab.com)

3월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	非윈도우	합계
103	83	2	0	0	0	0	0	10	0	208

[표1] 2005년 3월 유형별 신종 (변형) 악성코드 발견현황

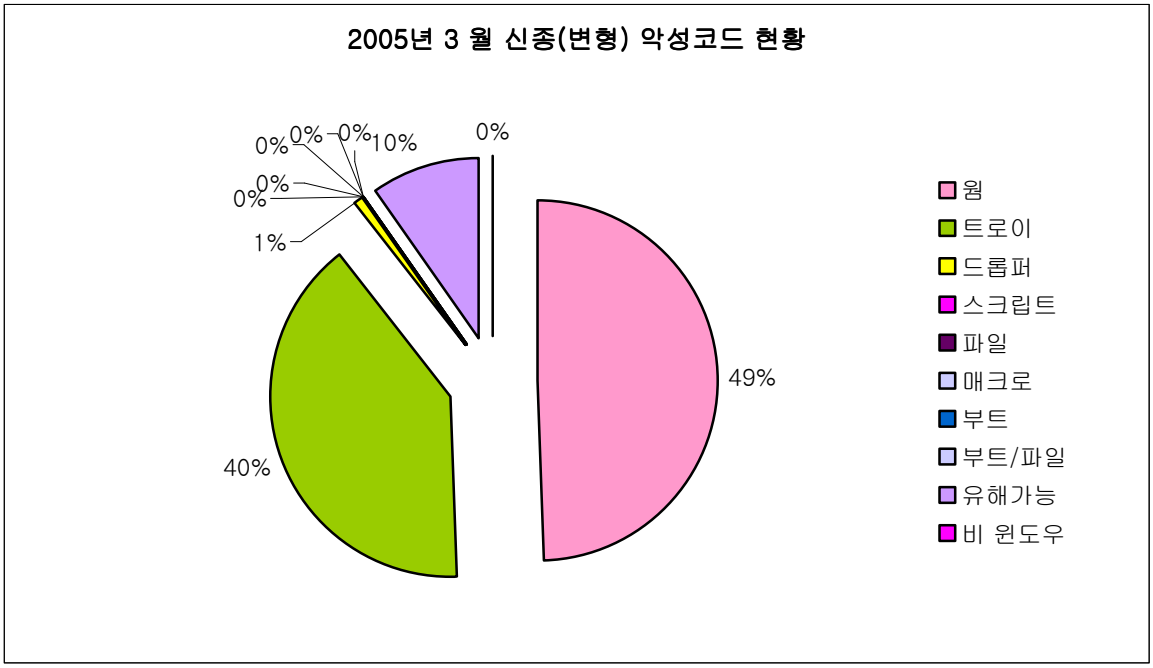
1, 2월과 비교하여 국내 접수된 악성코드의 수가 부쩍 줄었다. 특히 악성 아이알씨봇(IRCBot) 웜 변형이 많이 줄었는데 이것은 V3의 악성 아이알씨봇 진단율이 향상 되었기 때문으로 보여진다. V3의 악성 아이알씨봇 진단 향상의 성과는 단기간에 이루어진 것은 아니다. 악성 아이알씨봇에 대한 휴리스틱 진단기능 강화 등 오랜 기간에 걸쳐 준비해 온 결과이며, 그 결과로 작년 특정 시점부터 신고되는 악성 아이알씨봇 웜 변형이 줄어들고 있는 것을 알 수 있다.

그러나 악성 아이알씨봇 웜 변형의 발견이 감소한 원인에는 V3의 진단율 향상 외에도 다음의 2가지 원인이 더 있다고 유추해 볼 수 있다.

- 윈도우 XP SP2 사용자의 증가 (또는 업그레이드)
- 국가 정보보호기관들의 활동

위 두 가지 원인에 대해서 연구소에서 직접 파악해 본 것은 아니지만 윈도우 XP SP2의 경우 기본적으로 방화벽이 동작하며, 이 방화벽은 악성 아이알씨봇 웜 유입을 차단하는데 매우 효과적이라고 할 수 있다. 또한 국가 정보보호단체들은 악성 아이알씨봇 제작자들이 활동하는 아이알씨(IRC) 채널 및 서버를 찾아내어 이를 차단하는데 부단한 활동을 하고 있는 것으로도 알고 있다.

위와 같은 원인들로 악성 아이알씨봇 웜 수가 줄었다고는 하나 아직 안심하기는 이르다. 지금도 수많은 악성 아이알씨봇 웜이 제작되고 있으며 안티 바이러스 제품이나 보안 네트워크 장비를 회피 혹은 우회하려고 하기 때문이다.



[그림1]2005년 3월 신종(변형) 악성코드 비율

[그림1]은 3월 신종(변형)악성코드의 비율을 나타낸 것이다. 트로이목마 비율이 전체의 40%를 차지하고 있는데 이는 2월과 비교하여 배로 증가한 것이다. 또한 유해가능프로그램의 수도 배로 증가하였다. 3월 들어 크게 발견건수가 크게 증가한 트로이목마와 유해가능프로그램을 살펴보면 다음과 같다.

1) 트로이목마

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

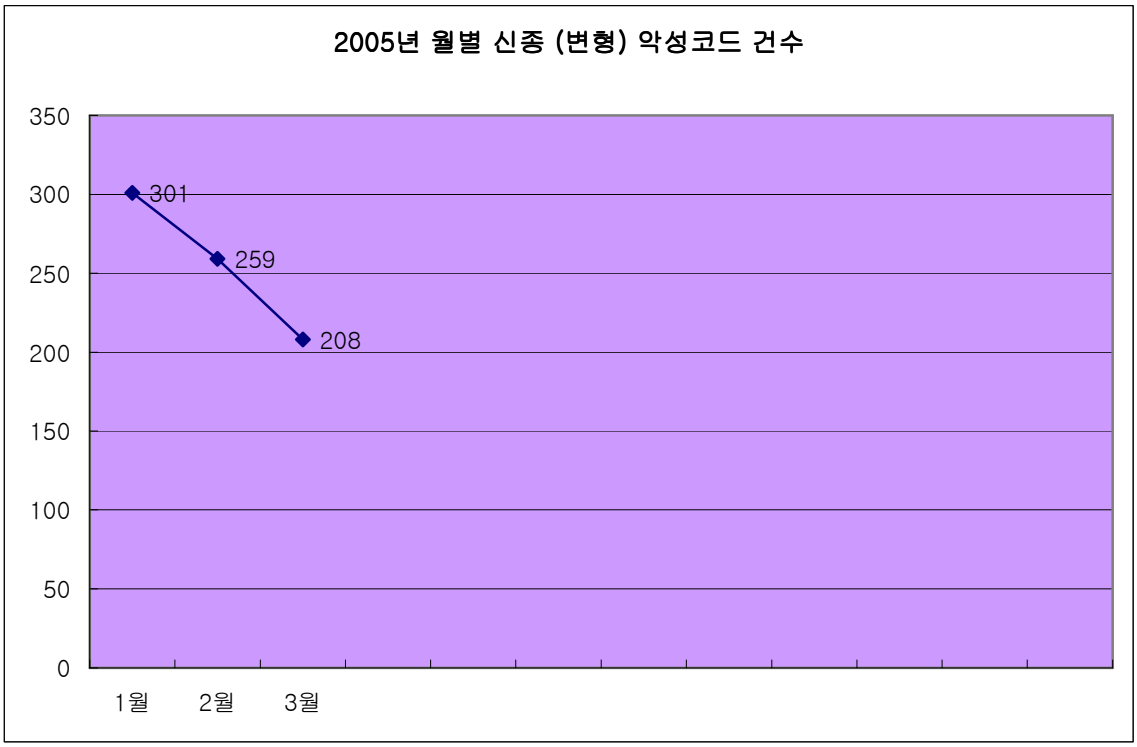
위 트로이목마들은 다른 악성코드와도 밀접한 관계를 가지고 있다. 보통 위 이름으로 명명된 트로이목마는 단독으로 실행되는 형태보다는 다른 악성코드나 스파이웨어에 의해서 연계되어 동작된다. 즉, 트로이목마 다운로더나 트로이목마 스타트페이지의 경우 스파이웨어들과 연동되며, 트로이목마 에이전트, 트로이목마 랭키, 트로이목마 스몰은 악성코드가 사용하는 프록시(Proxy) 서버기능을 가지고 있거나 이름이 명명되지 않는 은폐형 악성코드 등과 함께 동작된다. 이런 이유로 작년 하반기부터 트로이목마로 추가되는 위 진단명을 가진 악성코드 수가 부쩍 증가하고 있다.

2) 유해가능프로그램

- 하이드런(Win-AppCare/HideRun)
- 하이드윈도우(Win-AppCare/Hidewnd)
- 아이로퍼(Win-AppCare/Iroffer)
- 서브유(Win-AppCare/ServU)

3월에 증가한 유해가능프로그램으로는 위와 같으며, 이중 FTP 데몬으로 잘 알려진 서브유(ServU) 관련 유해가능프로그램이 가장 많았다. 정상 FTP 데몬이지만 악의적인 목적을 가진 사용자들로부터 코드가 압축되거나 수정되어 사용되는 형태가 이에 속한다. 하이드런과 하이드윈도우는 자신이 지정한 응용 프로그램의 윈도우를 보이지 않게 한다. 이는 사용자들이 감염내용을 눈치채지 못하게 하는데 그 목적이 있다. 아이로퍼의 경우도 정상적인 아이알씨(IRC) 관련 응용 프로그램이지만 악의적인 목적으로 사용되기 위해서 조작된 경우로 최근에는 변형 발견건수가 다소 줄어든 편이다.

다음은 월별 신종(변형) 악성코드 건수를 나타내고 있다. 위에서 언급한 것처럼 전체적인 신고 샘플수도 줄었다는 걸 알 수 있다.



[그림2]2005년 월별 신종(변형) 악성코드 발견 현황

올해 들어 계속 신종(변형) 발견이 감소한 수치를 보이고 있지만, 이는 단지 악성 아이알씨

봇 웜 변형 발견이 감소함에 따른 전체적인 수치의 감소일 뿐이다. 즉, 3월 들어서 이메일로 전파되는 마이탑 웜(Win32/Mytob.worm) 변형들이 지속적으로 보고되고 있으며, 트로이목마 발견수치 또한 지난달보다 증가했다는 것을 간과해서는 안된다.

3월 주요 신종(변형) 악성코드

이번 달 이슈가 되었던 주요 악성코드를 뽑는다면 당연히 마이탑 웜이 될 것이다. 그리고 MSN 메신저 관련 웜들과 은폐형 악성코드인 트로이목마 핵스도어(Win-Trojan/Haxdoor) 변형, 트로이목마 에이전트(Win-Trojan/Agent) 변형 등을 들 수 있다.

▶ 마이탑 웜(Win32/Mytob.worm)

이 글을 작성하고 있는 4월초에도 이 웜의 변형들이 계속 발견되고 있다. 현재까지 발견된 마이탑 웜 변형을 확인해 본 결과 총 18종이 2월말부터 4월초에 발견되었다. 이는 마치 작년에 기승을 부렸던 베이글 웜(Win32/Bagle.worm), 마이둠 웜(Win32/MyDoom.worm), 넷스카이 웜(Win32/Netsky.worm) 변형들의 발견속도와 유사하다. 이 웜은 이메일과 MS04-011 취약점을 이용하여 전파되며, 감염되면 특정 IRC 서버에 접속하여 파일 다운로드, 실행, 삭제 등의 명령을 수행하며, 자신이 포함된 이메일을 발송하게 된다. 그 외에도 변형에 따라 원형과 다른 취약점을 이용하기도 하며 관리목적 공유폴더를 통해 자신을 전파하기도 한다.

▶ 켈비르 웜(Win32/Kelvir.worm)

이 웜은 MSN 메신저를 이용하여 자신을 전파하며, 특정 호스트에서 악성 아이알씨봇 웜을 설치한다. 이러한 동작방식은 2월초에 많은 피해를 주었던 브로피아 웜(Win32/Bropia.worm)과 매우 유사하다.

▶ 수맘 웜(Win32/Sumom.worm)

이 웜 역시 MSN 메신저로 자신을 전파한다. 하지만 이 웜은 켈비르 웜이나 브로피아 웜과는 다소 다른 면이 있는데, 수맘 웜은 실행 후 윈도우 관련 레지스트리 정보를 변경하거나 특정 응용 프로그램을 실행하지 못하도록 한다. 또한 P2P 관련 공유폴더나 윈도우에서 기본적으로 공유되는 폴더에 자신의 복사본을 생성해두기도 한다.

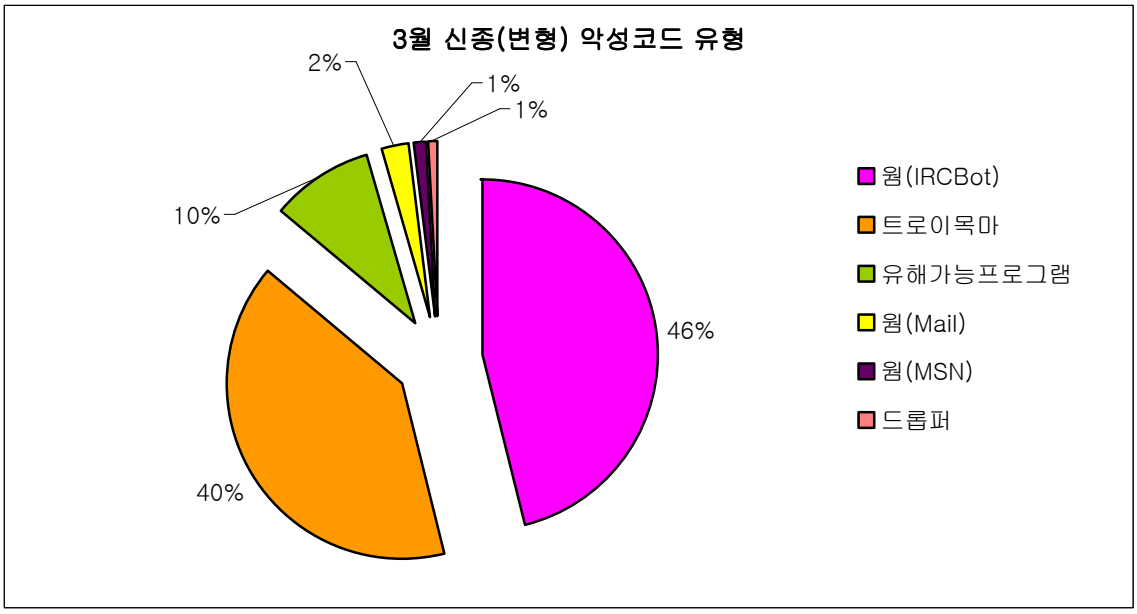
▶ 트로이목마 핵스도어(Win-Trojan/Haxdoor)

올해 들어 은폐형 악성코드에 대한 이슈가 부쩍 증가하였다. 특히 전통적인 악성코드 이외에 스파이웨어에서도 은폐형 증상이 자주 보고되고 있다. 트로이목마 핵스도어는 커널모드 은폐형 트로이목마로써 커널 관련정보를 조작하여 자신을 은폐하는 증상을 가지고 있다. 이 트로이목마 역시 많은 변형을 가지고 있다.

▶ 트로이목마 에이전트.243712(Win-Trojan/Agent.243712)

커널모드 기반의 은폐형 트로이목마인 에이전트.243712는 마이둠 웜에 의해서 다운로드되는 은폐형 트로이목마이다. 이 트로이목마는 프락시와 메일 릴레이 서버의 증상을 가지고 있다.

다음은 3월에 발견된 악성코드들을 유형별로 분류한 것이다.

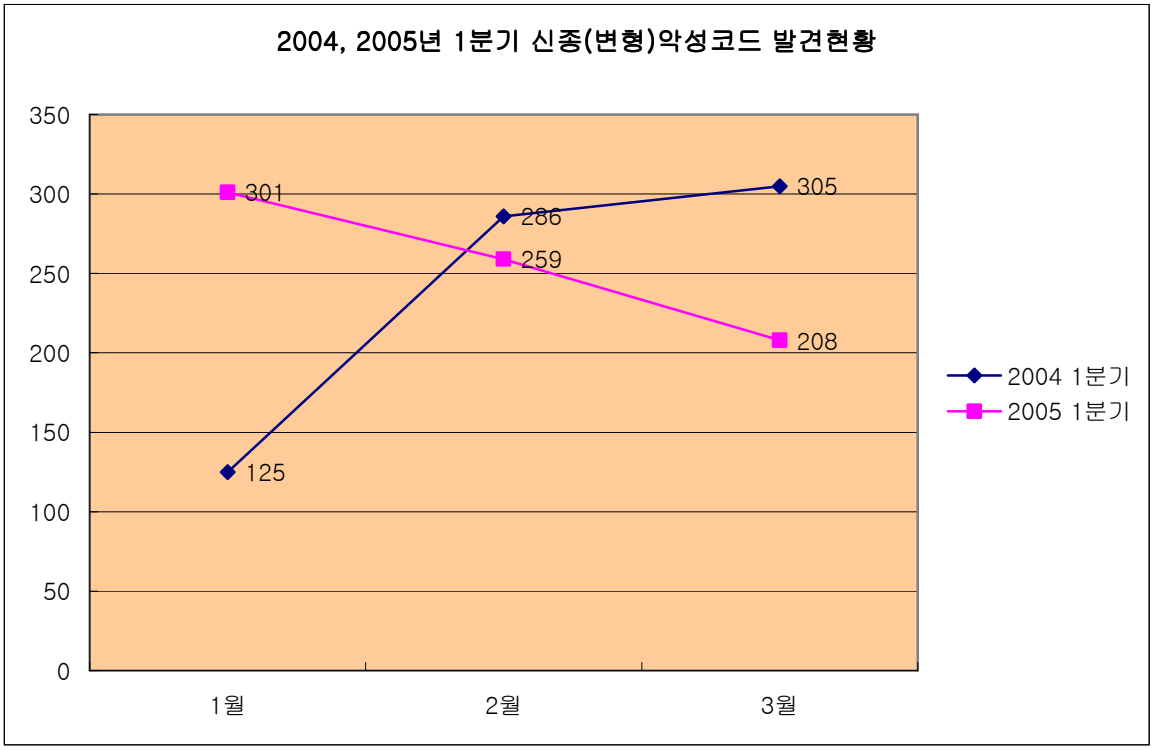


[그림3] 3월 신종 (변형) 악성코드 유형별 현황

3월에 국내에서 발견된 신종(변형) 웜은 크게 3가지 유형으로 나눠볼 수 있는데, [그림3]처럼 악성 아이알씨봇 웜, 이메일 웜, MSN 웜으로 분류할 수 있다. 드롭퍼 2종은 브로피아 웜 관련 악성 아이알씨봇 웜 그리고 은폐형 트로이목마와 관련이 있다.

2004년 1/4 분기 악성코드 통계 비교

작년 1/4 분기는 지금까지도 많은 피해를 입히고 있는 악성 아이알씨봇 웜 피해가 불거지기 시작한 시기이다. [그림4]를 보면 2004년 2월부터 국내에서 발견되는 신종(변형) 샘플이 급속히 늘어나는 것을 알 수 있다. 악성 아이알씨봇 웜 변형은 2004년 2월부터 지금까지 단일 변형으로는 유례가 없는 수 많은 변형들이 제작, 발견, 보고 되었다. 또한 이에 따라 제작 정보를 공유하는 커뮤니티 등이 활성화 되기 시작하였다.



[그림4] 2004, 2005년 1분기 신종(변형)악성코드 현황

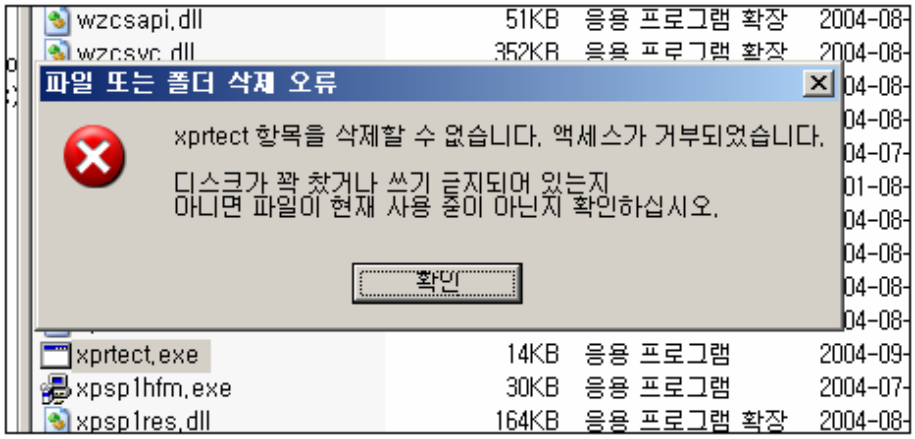
올해 1분기는 위에서 언급한 것처럼 악성 아이알씨봇 웜이 줄어들어 전체적으로 사용자로부터 접수되는 악성코드 수가 줄어든 것을 확인 할 수 있다. 하지만 그 수는 줄었어도 매일같이 발견되는 변형의 수와 피해문의는 좀처럼 줄어들 기세를 보이지 않고 있다.

작년 동기와 비교해볼 때 여전히 많은 수가 발견되고 있는 악성 아이알씨봇 웜, 그리고 큰 확산도를 가진 이메일 웜의 발견 등은 크게 달라지지 않았다. 더군다나 작년 이 기간 동안에는 많지 않았던 은폐형 악성코드의 이슈와 더불어 국외에서 많이 보고된 휴대폰 관련 악성코드까지 합한다면 줄어든 악성 아이알씨봇 웜의 숫자는 그리 큰 위안이 되지 않는다.

II. 3월 AhnLab 스파이웨어 동향

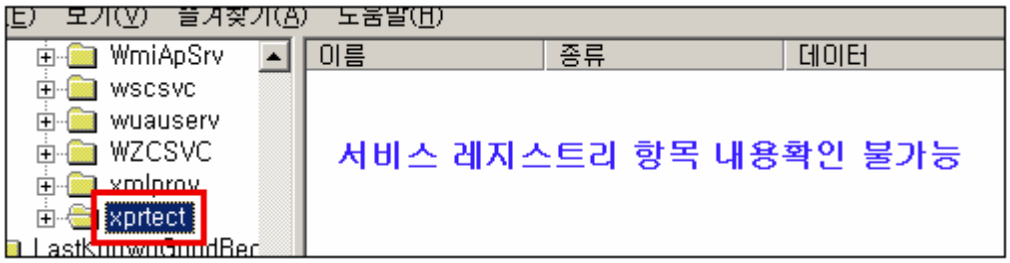
작성자 : 장혜윤 연구원(planet@ahnlab.com)

2005년 3월 작년에 이어 한글 키워드 시장을 둘러싼 경쟁이 다시 불붙기 시작했다. 이미 진출한 업체와 후발업체간의 시장쟁탈전이 재 점화된 것이다. 한글 키워드 서비스는 MS 익스플로러 주소창에 한글을 입력하면 중간에서 이를 영문 도메인으로 바꾸어 원하는 사이트로 연결해주는 서비스이다. 예를 들어 안철수연구소 홈페이지에 접속하고 싶을 때 주소창에 'www.ahnlab.com'이라는 영문 도메인 주소를 입력하는 대신 간단히 한글로 '안철수연구소'라고만 쓰면 안철수연구소 홈페이지에 접속이 가능한 것이다. 국내에서 제공하고 있는 한글 키워드 서비스에는 두 가지 방식이 있다. 하나는 초고속인터넷 업체들과의 제휴를 통해 DNS서버[1]에서 한글 키워드를 영문 도메인으로 바꿔주는 방식이고, 다른 하나는 입력된 키워드를 영문도메인으로 바꿔주는 플러그인을 설치하는 방식이다. 플러그인 설치 방식은 시장점유율을 높이기 위해 업체들간에 사용자의 컴퓨터에 상대 경쟁업체 플러그인의 실행을 방해하는 프로그램을 배포하는 등의 치열한 경쟁을 보여왔는데, 최근에는 한글 키워드 플러그인을 설치하는 스파이웨어까지 등장하는 양상을 보이고 있다. 스파이웨어 아이가드(Win-Spyware/iGuard)가 그것인데, 이는 Xprtect.exe 외 4개 파일을 사용자 동의 없이 커뮤니티 게시판 등을 통해 다수 사용자들의 Win98, NT계열(Win2000, WinXP) 시스템에 배포하여 설치된 것으로 추정된다. 설치된 파일들은 xprtect.sys 및 xprtect.vxd의 서비스에 등록되는 드라이버 파일이며 [그림1]과 같이 사용자 또는 스파이웨어 제거프로그램이 스파이웨어 아이가드를 제거할 수 없도록 하는 파일 보호 기능을 가지고 있다.



[그림1] 파일 보호 기능으로 인해 파일을 제거할 수 없는 화면

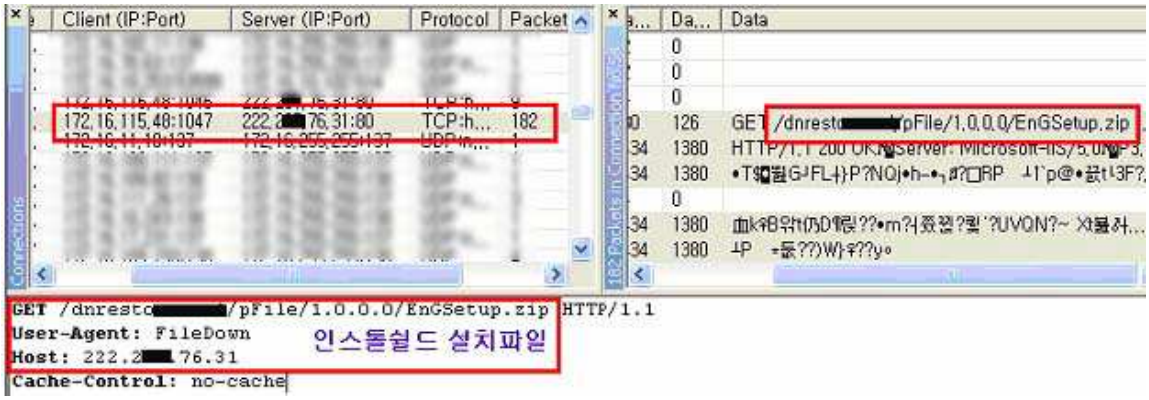
[1] DNS (Domain Name System)는 인터넷 도메인 이름들의 위치를 알아내기 위한 IP 주소로 바꾸어주는 시스템이다. 도메인 이름은 인터넷 주소로서 사람들이 기억하기 쉽고, 의미있게 붙인 이름이지만, 인터넷에서 어떤 컴퓨터를 실제로 찾기 위해서는 숫자 체계로 된 IP 주소가 필요하다.



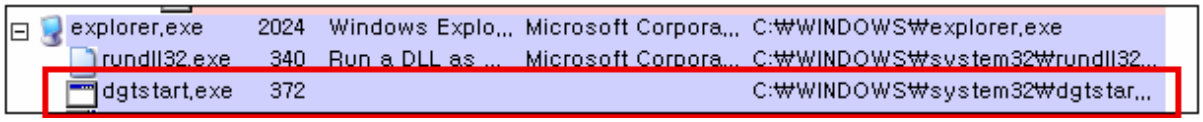
[그림2] xprtect 서비스 레지스트리 항목 내용 확인이 불가능한 화면

또한 [그림2]와 같이 사용자로부터 서비스 레지스트리 항목의 내용확인이 불가능하다.

설치된 스파이웨어 아이가드는 특정 키워드 및 특정 사이트 접속시에 인스톨 쉴드로 된 설치파일(EnGSetup.zip)을 다운로드 한 후 키워드 인터넷 한글접속 도우미를 설치(dgstart.exe)한다.



[그림3] 스파이웨어 원격지 서버에 접속하여 설치파일 다운로드하는



[그림4] 설치후 실행된 키워드 인터넷 한글접속 도우미

현재, 경쟁업체들마다 각각 다른 방식으로 한글 키워드 서비스를 제공하면서 같은 한글 키워드를 주소창에 입력하더라도 업체별로 서로 다른 홈페이지에 접속되는 현상이 생겨 기대를 모았던 한글 키워드 서비스는 사용자들에게 외면을 받고 있다. 한글 키워드가 실효성을 갖기 위해서는 영문 도메인처럼 누구나 한글 키워드를 입력하면 일정한 규약에 의해 항상 같은 사이트로 이동해야 하지만, 업체마다 키워드 별 등록되어 있는 사이트가 틀리기 때문에 주소로서의 가치가 전혀 없다. 한글이 인터넷에서 통용되는 국제주소체계가 아니기 때문에 한글 키워드는 영문 도메인처럼 고정될 수 없다. 그럼에도 불구하고 사용자들이 그 동안 불편을 거의 느끼지 못했던 것은 국내 한글 키워드 서비스를 제공하는 업체가 적고, 특정 업체에서

독점해왔기 때문이다. 하지만 최근 많은 경쟁업체가 출현하면서 상황이 급변했다. 한글 키워드 선점 경쟁이 벌어지면서 어떤 업체의 방식을 이용하느냐에 따라 같은 한글 키워드를 입력해도 이동되는 사이트 달라지는 현상이 발생하고 있는 것이다.

이와 같이 업체들간 대립이 벌어지고 있는 동안 그 피해는 고스란히 사용자들에게 돌아오고 있다. 시장이 경쟁체제가 되면서 오히려 이용자들의 불편이 늘어나는 상황이 벌어지고 있는 것이다.

III. 3월 시큐리티 동향

작성자 : 이정형 주임연구원(jungh@ahnlab.com)

이번 달에는 인터넷 익스플로러의 MSHTML.DLL Parse 부분의 CSS Handling Buffer Overflow(MS04-038) 취약점 공개소식과 지속적으로 국내 웹 해킹이 대량으로 이루어지는 문제점, 해결책을 살펴보기로 한다.

MS IE MSHTML.DLL CSS Handling Remote Buffer Overflow Exploit

CSS(Cascading Style Sheet)는 웹 문서(HTML)에 전체적 또는 부분적으로 적용가능하고, 웹 페이지를 다양하게 설계하고 수시로 변경하는데 많은 제약을 해결해 주는 스타일 시트이다. W3C의 http://www.w3.org/Style/CSS/ 에 정의가 되어있으며 홈페이지 제작에 필수적으로 사용되고 있다.

이 취약점은 인터넷 익스플로러에서 웹페이지를 Parsing할 때 사용되는 MSHTML.DLL의 CSS Parse 부분에 버퍼를 체크하지 않아 버퍼 오버플러우가 발생하는 취약점이다.

악의적인 공격자는 CSS 파일을 조작하여, 관리자의 공격을 획득할 수 있으며, 악의적인 웹 사이트 방문 시에도 관리자 권한이나 임의의 공격을 받을 수 있다. 조만간 이 취약점을 이용한 웜이 출현할 것으로 보여진다. 보안 패치를 하지 않은 사용자이라면 MS04-038 패치를 적용하도록 하여 미리 예방해 두기를 권장한다.

현재 인터넷 익스플로러에서는 보안패치가 아직 발표되지 않은 취약점들도 있다. 따라서 신뢰되지 않은 사이트는 접속하지 않는 것 또한 취약점을 이용한 악성코드 피해 예방방법 중의 하나라 할 수 있다.

지속적인 국내 웹 해킹 대량 변조 문제점과 해결책

올해 초 다수의 국내 웹 서버 해킹 사건이 발생한 이후에도 지속적으로 웹 어플리케이션 취약점을 이용한 국내 웹 서버 해킹이 이루어지고 있다.

필자는 몇 년 전에 국내 게시판의 보안 문제점을 다룬 적이 있었다. 웹 해킹 공격이 계속 이루어지는 이유는 웹 어플리케이션의 취약점과 해당 서버의 취약점에 기인한 것으로 크게 나눌 수 있다..

▶ 웹 어플리케이션의 취약점을 이용한 웹 해킹

게시판 또는 포럼 등의 웹 어플리케이션을 통해 공격을 당하는 경우, 방화벽(Firewall)이 설치되어 있더라도 무용지물이 되기 십상이다.

국내 많은 중요 기관, 기업들이 국내에서 공개된 게시판들을 사용한다. 최근 보안 문제를 제공하는 원인 중 상당부분이 바로 취약점을 가지고 있는 국내 게시판, 포럼 등의 웹 어플리케

이션이다.

그렇다면 웹 어플리케이션 취약점 종류 및 해결 방법에 대해서 알아보자

1) upload 취약점

.php .ph 등의 file을 업로드 한 후 bindshell을 통해 웹서버 권한을 획득하는 기법이다.
이러한 스크립트가 파일이 저장되는 디렉토리에 대해서 소스처리 하는 방법이다.
아파치(Apache) 설정 예제는 다음과 같다.

```
<DirectoryMatch "^/home/.*/data">
  AddType application/x-httpd-php3-source .phps .php .ph .php3 .cgi .sh
.pl .html .htm .shtml .vbs .ins
  AddType application/x-httpd-php-source .phps .php .ph .php3 .cgi .sh
.pl .html .htm .shtml .vbs .ins

  <Files ~ ".*₩.ph$">
    Order allow,deny
    Deny from all
  </Files>
</DirectoryMatch>
```

2) setup file 노출

아파치의 httpd.conf에 다음 줄을 추가하여 패스워드, 데이터베이스 등의 설정파일이 노출되는 문제를 해결할 수 있다.

AddType application/x-httpd-php .php .php3 .ph .inc

3) 디렉토리, 파일 인가(Directory, File Permission)

웹 어플리케이션 설치 시 Directory 및 해당 File이 모든 유저에 대해 쓰기권한이 적용되는 경우가 존재한다. nobody를 제외한 유저들의 쓰기 권한을 제거하고, 해당 글이 저장되는 파일에 대한 인가(permission)을 검사한다

4) shell 실행 함수 및 파일 오픈관련 함수

system(), passthru(), exec(), popen(), escapeshellcmd(),` `(Backticks) 및 fopen(), include() 함수 등을 사용할 경우, 메타캐릭터 문자인 .<>*|'&;$!#()[]{}:"/^₩n₩r 를 제거해 주도록 하자

5) 버퍼 오버플로우(Buffer Overflow)

아래와 같은 종류의 함수를 사용할 때는 버퍼 크기에 주의하도록 한다.

gets (),getenv(), strcpy (), strcat (), sprintf (),
fscanf (), scanf (), sscanf (), vscanf(),vsscanf (),
vfscanf(),vsprintf (),realpath (), getopt (), getopt_long(),
getpass (), streadd (),strecpy (), strtrns ()

되도록이면 bcopy(), fgets(), memcpy(), strncpy(), snprintf(), strccpy(), strcadd(), vsnprintf()으로 대체해서 사용하도록 한다

6) SQL Injection

웹 어플리케이션은 보통 데이터베이스와 연동이 되는 경우가 많다.
SQL Injection은 사용자의 입력이 필요한 곳에 SQL Query 문을 넣어 악의적인 명령어를 수행하는 기법이다. 이에 대한 해결책으로는 사용자의 입력이 필요한 부분에 <>*|'&;$!#()[]{}:"/^₩n₩r 등의 쉘 메타캐릭터를 사용하지 못하도록 제거하는 것이다.

PHP의 설정화일인 php.ini에서는 보안을 강화하는 옵션이 존재한다. 다음 옵션을 조정하여 보안을 강화시킨다.

allow_url_fopen = Off
magic_quotes_gpc = On
register_globals = Off

현재 국내에서 사용되어지는 KorWeblog 그누보드, 제로보드, 테크노트등의 취약점이 존재하므로, 보안패치를 적용하지 않은 사용자들은 즉시 보안패치를 적용하도록 하자.

▶ 서버상의 취약점 및 해결 방법

mod_php, mod_perl, mod_python 등은 아파치 모듈로 스크립트 언어가 동작할 수 있다.
해당하는 모듈에 취약점이 발생하면 웹 서버 권한을 빼앗기게 되며, 이를 이용하여 서버에 접근할 수 있다. 몇달전 PHP의 Remote Buffer Overflow 취약점이 나온 이후, 크래커들이 이 취약점을 이용하여, 웹 서버를 공격하는 것으로 보여진다. PHP 버젼을 체크한 후에 http://www.php.net의 최신버전으로 반드시 패치를 적용해야 한다.
기타로는 McAfee Antivirus에서 LHA 압축라이브러리의 Buffer Overflow와 Symantec Gateway Security 제품의 DNS Cache Poisoning 취약점, Symantec Norton AntiVirus에 관한 취약점 소식이 있었다. 해당 업체 홈페이지에 접속하여 보안패치를 적용시키면 해결이 가능하다.

다시 한번 강조하지만, 웹 해킹 등의 피해를 예방하기 위한 가장 기본적인 보안은 해당 제품

의 패치임을 잊지 않는 것이 중요하겠다.

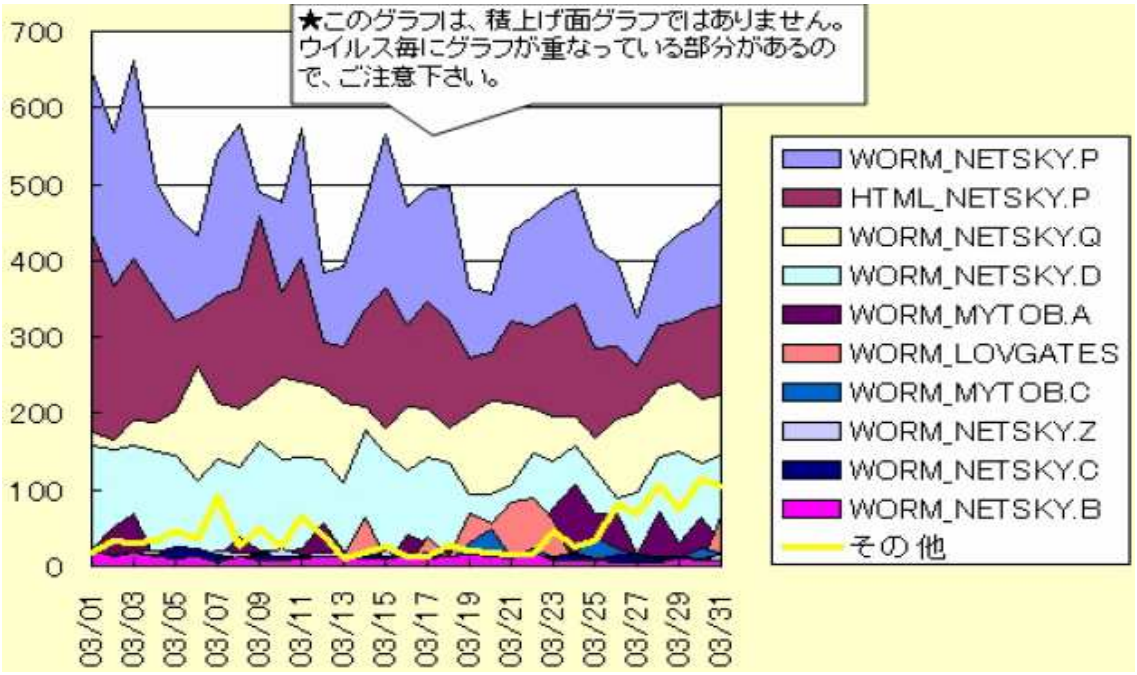
Ⅳ. 3월 세계 악성코드 동향

3월 전세계 악성코드 동향은 단연 메일로 전파되는 매스메일러(Mass Mailer)가 많은 확산을 보이고 있는 것으로 분석되며 국가별 악성코드 순위에서도 대부분 매스메일러들이 높은 순위를 차지하고 있었다. 그러나 세부적으로 분석해 본다면 일본은 여전히 넷스카이 웜이 많은 확산을 보이고 있지만 중국의 경우에는 오히려 감소의 추세를 보이고 백쯔 웜의 확산이 높은 편으로 분석된다. 또한 이러한 극동 아시아지역과는 달리 유럽 지역은 자피 웜과 마이둠 웜의 확산이 높은 편이었다.

(1) 일본의 악성코드 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

3월 한달 동안 일본의 악성코드 동향과 관련하여 가장 큰 특징은 넷스카이 웜(Win32/Netsky.worm)의 지속적인 확산과 마이탑 웜(Win32/Mytob.worm) 변형이 확산된 점이다. [그림1]은 일본의 IPA에서 관측한 3월 한달 동안의 악성코드 탐지현황을 표로 나타낸 것이다.



[그림1] 악성코드의 종류별 확산도

[그림1]에서 나타난 것처럼 넷스카이 웜의 여러 변형들이 많이 확산되고 있으며 특히 넷스카이.P(Win32/Netsky.P, V3 진단명 Win32/Netsky.worm.29568)형의 경우 다른 변형들과 비교하여 매우 많은 감염 피해를 주고 있는 것으로 나타났다. 마이탑 웜 또한 많이 확산되고

있는 것을 알 수 있는데 제작되어 배포된 기간이 짧고 아직 변형이 많지 않은 관계로 마이둠 웜이나 베이글 웜과 같이 잘 알려진 매스메일러에 비해 전체적인 감염 피해 정도는 낮은 상태이나 단일 악성코드로는 더 많은 트래픽을 발생시키고 있는 것으로 볼 수 있다. 따라서 새로운 변형들이 지속적으로 등장할 경우 사용자들의 감염 피해가 점점 늘어날 것으로 예상된다.

악성코드 피해 동향

2005년 3월 한달 동안 일본에서 가장 많이 확산되어 피해를 입힌 악성코드는 넷스카이 웜이다. [표1]은 일본 IPA(www.ipa.co.jp)에서 발표한 3월 한달 동안의 악성코드 감염 통계이다. 전월과 마찬가지로 넷스카이 웜이 가장 많은 감염 피해를 기록하고 있는 것을 알 수 있다.

Win32/Dos 바이러스		매크로 바이러스		스크립트 바이러스	
악성코드명	피해 건수	악성코드명	피해 건수	악성코드명	피해 건수
Win32/Netsky	1,262	XM/Laroux	17	VBS/Redlof	62
Win32/Bagle	484	W97M/Ethan	4	VBS/Loveletter	16
Win32/Mydoom	399	Tristate	4	Wscript/Fortnight	8
Win32/Lovgate	292	XF/Sic	3	VBS/Soraci	3
Win32/Klez	249	X97M/Squared	2	VBS/Freelink	2
Win32/Zafi	192	W97M/Opey	1	VBS/Internal	2

[표1]악성코드 피해 현황(출처:일본IPA)

표에는 나오지 않았으나 최근 발견된 마이탑 웜의 경우 피해 건수는 147건으로 3월에 사용자들에게 많은 피해를 주었다. 마이탑 웜은 2005년 2월 말에 최초로 발견된 이후 현재까지 여러 형태의 변형들이 발견되고 있는 메일을 통해 전파되는 악성코드이다. 전체 감염 피해 건수가 전월에 비해 늘어난 점도 주목할 만 하다. 2월의 경우 전체 감염 피해 신고는 4,150건이었으나 3월의 경우 4,846건으로 약 16% 정도가 증가했다. 감염 피해 증가의 원인은 넷스카이 웜의 감염 피해 건수가 전월에 비해 늘어났고 마이탑 웜 등 새로운 메스메일러가 제작되어 배포된 점 등으로 생각된다.

악성코드 감염 경로별 통계

3월 한달 동안 일본에서 악성코드 감염의 경로로 가장 많이 이용된 매체는 메일이다. 한 해 동안 발견되는 악성코드들 중에서 매스메일러가 차지하는 비율은 매우 낮고 실제로 사용자들에게 직접 감염되는 악성코드의 종류는 한정되어 있음에도 불구하고 매스메일러를 통한 감염 피해는 줄어들지 않고 있다. 인터넷을 사용하는 대부분의 사용자가 이용하는 매체이고 메일 사용시 감염 예방을 위한 지식이 없는 상태라면 첨부된 파일을 실행하여 감염이 될 가

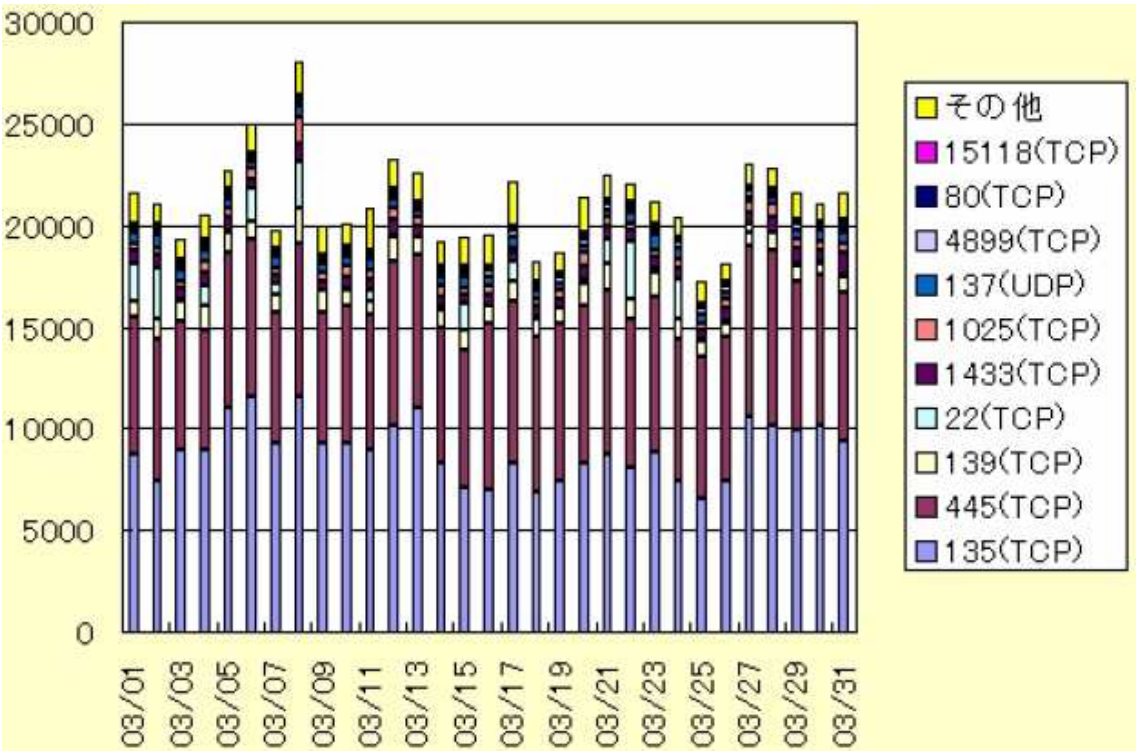
능성이 항상 존재하기 때문에 감염 예방을 위한 사용자들의 지속적인 교육이 필요하다.

감염 경로	감염 건수					
	2005년 3월		2005년 2월		2004년 3월	
메일	4,780	98.6%	4,111	99.1%	3,956	98.6%
다운로드	2	0%	0	0%	12	0.3%
외부의모체	2	0%	0	0%	15	0.4%
네트워크	54	1.1%	39	0.9%	12	0.3%
기타	8	0.2%	0	0%	17	0.4%

[표2] 악성코드 감염 경로 통계

일본 네트워크 트래픽 현황

[그림2]는 3월 한달 동안의 네트워크 트래픽 현황을 표로 나타낸 것이다. TCP 135 포트와 TCP 445 포트를 이용한 트래픽이 매우 많은 것을 볼 수 있다. 해당 포트들은 윈도우 OS에서 사용되는 포트들로써 서로 다른 시스템간의 인증을 처리하는 것과 관련되어 사용된다. 그러나 악성 아이알씨봇과 같은 네트워크를 통해 전파되는 웜의 취약점을 이용한 공격에 사용되는 경우 또한 빈번하게 발생하고 있다. 최근 제작되어 배포되는 웜들은 패스워드를 크랙하거나 OS의 취약점을 이용해 버퍼 오버플로우를 발생시켜 권한을 획득한 후 감염시키는 기능을 가지고 있는 경우가 대부분이므로 주의가 필요하다.



[그림2] 네트워크 트래픽 현황

(2) 중국의 악성코드 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

3월 중국 악성코드의 동향은 1월과 2월에 이어서 백쯔 웜(Win32/Bagz.worm)이 1위를 유지하고 있다. 그리고 라이징과 중국 컴퓨터바이러스긴급대응센터(이하 CNCVERC)의 3월 악성코드 TOP 5에는 새로운 악성코드 2개가 순위권에 진입하였다. 그럼 3월에는 어떠한 악성코드가 순위권에 진입을 하였는지 그리고 새로 발견되었는지 살펴보도록 하자.

악성코드 TOP 5

순위 변화	순위	Rising
-	1	TrojanDroper.Worm.Bagz
-	2	Backdoor.Rbot
New	3	Worm.MSN.Bropia
↓ 1	4	Worm.Agobot
New	5	Trojan.Win32.StartPage

[표1] 2005년 3월 Rising 악성코드 TOP 5

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

순위 변화	순위	CNCVERC
-	1	Worm_Netsky.D
New	2	Worm_AgoBot
New	3	Worm_Bropia.F
↓ 1	4	Worm_Bbeagle.J

[표2] 2005년 3월 CNCVERC 악성코드 TOP 4

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

[표1]과 [표2]는 중국 백신 업체인 라이징(Rising)과 CNCVERC의 악성코드 TOP 5이다. 우선 라이징의 TOP 5부터 살펴본다면 새로운 악성코드 2건이 새롭게 순위에 기록되었다. 1월말에 최초 등장한 브로피아 웜(Win32/Bropia.worm)이 3위로 기록되었다. 그러나 QQ 메신저라는 로컬 업체에서 개발한 메신저를 많이 사용하는 중국에서 MSN 메신저로 전파되는 브로피아 웜의 감염율이 높다는 것은 특이점으로 분석된다. 5위로 기록된 스타트페이지(Win-Trojan/StartPage)는 3월 이전부터 조금씩 신고 건수가 증가하는 것으로 분석되었지만 3월에 이르러서는 드디어 순위권에 진입할 정도로 감염신고가 증가하였다. CNCVERC의 TOP 5도 3월에 이르러서는 전반적인 순위 변화가 있었다. 순위의 변화는 라이징과 유사하게 아고

봇(Win32/AgoBot.worm)과 브로피아 웜이 순위에 새롭게 랭크되었다. 두 악성코드 TOP 5의 순위를 비교해보면 중국내에서 악성 봇과 브로피아 웜의 전반적인 감염율이 높은 것을 알 수 있다.

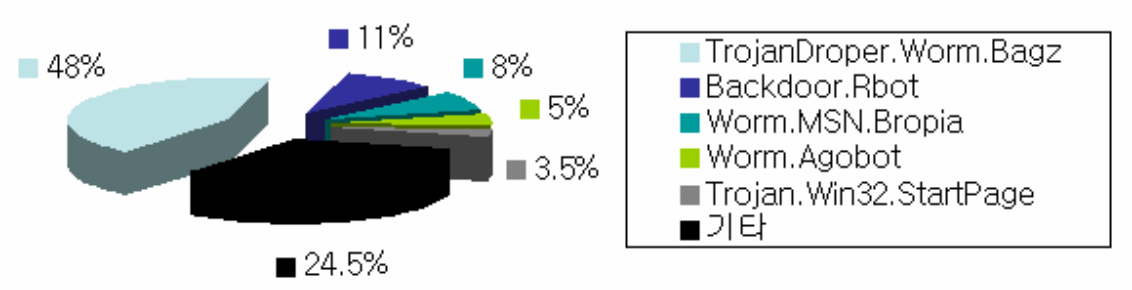
주간 악성코드 순위

순위	1주	2주	3주	4주
1	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz
2	Backdoor.PcShare.2005.a	Worm.MSN.Bropia	Backdoor.Rbot	Backdoor.Rbot
3	Backdoor.Rbot	Backdoor.Rbot	Worm.LovGate	Trojan.Win32.StartPage
4	Backdoor.Netbot	Worm.Agobot	BackDoor.SdBot	Backdoor.Agobot
5	Worm.Agobot	Backdoor.Huigezi	Trojan.PSW.QQPass	BackDoor.SdBot

[표3] 2005년 3월 Rising 주간 악성코드 순위

주간 악성코드 순위 변화를 살펴보면 4주 동안 백쯔 웜이 1위를 차지하고 있는 것을 잘 알 수 있으며 악성 봇 변형들 역시 순위권 내에 포함되어 있다. 스타트페이지는 3월 마지막 주에 주간 순위에 랭크되었으나 TOP 5에도 등장할 만큼 많은 감염 보고가 있었던 것으로 분석되어 중국 내에서도 트로이목마로 분류할 수 있는 애드웨어와 스파이웨어들의 감염 신고도 점차 증가하고 있는 것으로 분석된다.

악성코드 분포



[그림1] 2005년 3월 중국의 악성코드 분포

3월 중국 악성코드 분포를 살펴본다면 전체의 절반이 조금 못 미치는 48%를 백쯔 웜이 차

지하고 있어 백쯔 웜이 중국 내에서는 아직도 높은 감염율을 보이고 있는 것을 잘 알 수 있다. 그 외에 악성 봇 변형인 알봇과 아고봇이 각각 11%와 5%를 차지하고 있어 지난 1월과 비교한다면 전체 분포에서 다소 감소한 것으로 보여진다. 그리고 전체 분포도 면에서 24.5%를 차지하고 있는 기타는 대부분이 트로이목마 형태이며 개개의 악성코드 수치상으로는 높지 않은 것으로 미루어 다양한 악성코드들이 많이 등장한 것으로 해석할 수 있다. 그러나 백쯔 웜이 전체의 48%를 차지하고 있는 것으로 보아 당분간은 백쯔 웜의 확산이 지속될 것으로 보인다.

(3) 세계 악성코드 동향

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

2005년 1월, 2월에 이어 3월에도 순위에는 큰 변화가 없다. 여전히 자피 웜(Win32/Zafi.worm) 변형, 넷스카이 웜(Win32/Netsky.worm) 변형, 마이둠 웜(Win32/MyDoom.worm) 변형 등이 대부분의 순위를 차지하고 있다. 자피 웜은 아시아 지역에서는 피해 보고가 거의 없지만 유럽 지역에서는 여전히 많은 감염 보고가 되고 있다.

한국에서 감염 보고가 네번째로 높은 새서 웜(Win32/Sasser.worm.15872)이 다른 지역에서는 순위에 들지 못한 것도 흥미롭다. 새서 웜은 패치 되지 않은 윈도우 2000 이나 윈도우 XP 에서 감염되므로 한국에는 여전히 패치를 하지 않은 시스템이 많은 것으로 보인다. 하지만, 새서 웜은 한글 윈도우에 감염 시도 할 때 종종 시스템이 꺼지는 버그가 나타나므로 사용자들이 감염 사실을 인지할 가능성도 높으므로 상대적으로 감염 보고가 높을 수도 있다.

3월은 마이탑 웜 변형(Win32/Mytob.worm)이 계속 등장해 사용자를 괴롭혔지만 변형 중 하나만 캐스퍼스키 연구소(Kaspersky Lab) Top 20에서 4위를 차지했다.

새로운 악성코드가 등장하지 않는 이상 현재의 순위 구조를 당분간 지속될 것으로 보인다.

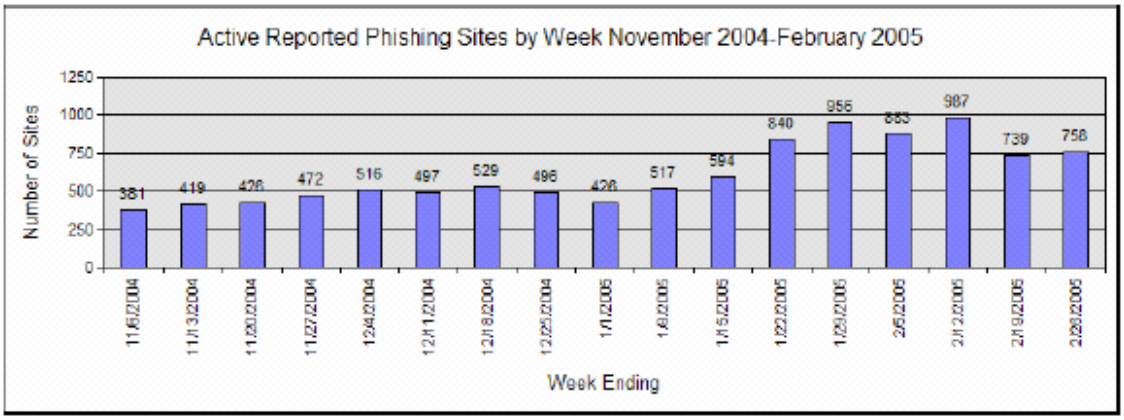
V. 이달의 ASEC 컬럼 – 피싱에 이은 '파밍' 과연 또 다른 위협의 도전인가?

작성자 : 정관진 주임연구원(intexp@ahnlab.com)

피싱(Phishing)은 작년부터 신종 인터넷사기수법으로 언론에 크게 대두되며 새로운 보안 위협의 하나로 조명 받기 시작했다. 인터넷의 대중화와 함께 일반 사용자들 또한 피싱의 위협에 노출되어 피해의 대상이 확대된 것이다. 이것은 과거의 피해대상이 한정되었던 것에 비해 초고속인터넷망의 가속화와 IT 인프라의 급격한 증가가 일반 개인 사용자들의 인터넷 연결 기회를 증대시켜 피해 대상의 범위가 넓어지고 있는 것이다.

피싱이란 사회공학적 기법[1], 기술적 속임수를 이용하여 사용자의 개인 신상정보 또는 계좌정보와 같은 금융정보를 빼내가는 수법으로 정의될 수 있다. 현재 피싱 공격으로 가장 많이 이용되는 방법은 불특정 다수를 대상으로 조작된 이메일을 전송하여 사용자가 피싱 사이트를 방문하게끔 유도하여 사용자의 입력된 정보를 얻는 것으로, 피싱 사이트는 사용자가 의심하기 어렵게 정교하게 작성되어 있는 경우가 보통이다.

[그림1]은 안티피싱 워킹그룹(Anti-Phishing Working Group)에서 발표한 자료로 피싱 사이트가 전반적으로 꾸준한 증가추세를 나타내고 있는 것을 알 수 있다. 2월에 발표된 보고서에 따르면 전체 피싱 중 금융기관을 대상으로 한 것이 약 80% 가까이 되며 6-7개의 특정 브랜드를 사칭하는 것이 80% 이상이 될 만큼 현재는 특정 브랜드의 금융기관이 주 목표 대상이 되고 있다.



[그림1] 2004년 11월 ~ 2005년 2월 사이에 보고된 피싱 사이트 추이

피싱 형태는 갈수록 더욱 교묘해지고 있는데 사용자가 의심을 가지지 못하도록 웹페이지를

[1] 사회공학적 기법(Social Engineering)이란?
친근하거나 호기심을 끌만한 내용으로 사람의 심리를 이용하는 방법이다.

정교하게 만들거나 취약점을 이용한 위조된 메일 또는 사이트를 만들어 쉽게 인지하지 못하도록 복합적이고도 기술적인 방법들이 많이 사용되고 있는 추세이다.

이와 같은 행보는 앞으로 더욱 늘어날 것으로 추정되는데 과거 공격방법들이 현재까지 변화해온 형태를 보면 단순하면서도 많은 지식을 요구하였지만 공격은 더욱 고도화되고 그 방법 자체는 쉬워지고 있다는 것을 보면 피싱 또한 이와 같은 트렌드를 따라갈 것이다.

최근 이러한 트렌드를 반영하듯이 피싱 공격 유형중의 하나로 '파밍(Pharming)' 이라는 것이 등장해 또 다시 언론의 주목을 받고 있다. 새로운 형태의 사기수법으로 보여지고 있지만 파밍은 과거에 해킹기술로 소개되었던 방법을 이용한 형태이며 기술적 방법에 대한 차이만을 가지고 있기 때문에 피싱의 범주로 보는 것이 올바르다. 즉, 피싱 공격에는 위조된 이메일 또는 홈페이지를 이용한 기술적 방법들이 이용되고 있지만 파밍은 DNS(Domain Name System) 또는 프록시 서버(Proxy Server)의 주소를 직간접적으로 변조하여 사용자측에서 보면 피싱 보다 더욱 쉽게 속아 넘어갈 수 있는 가능성을 높여 주고 있다. 파밍으로 이용될 수 있는 방법을 다음과 같이 정리해 볼 수 있다.

- DNS 주소의 변조
- 클라이언트 호스트 파일 변경
- 클라이언트 DNS 서버설정 주소 변경
- 등록된 도메인의 정보 변경
- 프록시 서버 이용

* 클라이언트의 호스트 파일 또는 DNS 서버설정 변경은 트로이목마와 같은 악성코드에 의해 변경될 수 있다.

파밍의 기본적인 토대는 사용자의 개입 없이 쉽게 유도할 수 있도록 주소변경에 중심을 두고 있고 'DNS 주소의 변조'가 가장 일반적인 형태이다. DNS는 사이트에 접속할 때 흔히 입력하는 도메인주소를 IP 주소로 변경해 주거나 또는 그 반대의 역할을 수행하는 기능을 가지고 있다. 이것을 필요로 하는 이유는 실제 네트워크 상에서의 통신은 IP를 통해 이뤄지고 있고 우리는 IP 주소를 다 기억할 수 없기 때문에 DNS 라는 것을 이용하여 원하는 곳을 쉽게 기억하고 찾아 들어가는데 이용하는 것이다.

기존의 피싱 공격은 유사한 이름의 도메인 주소를 이용하거나 정상적인 사이트를 통한 리다이렉트, 정교한 위조 페이지 등을 이용하여 위조된 피싱 사이트로 유도하였으나 사용자가 주의 깊게 살펴보면 피싱 사이트를 인지할 수 있는 부분도 있었다. 하지만 이렇게 DNS 주소를 변경시키게 되면 사용자의 판단은 더욱 어려워지고 믿고 넘어갈 가능성이 높아진다. 이와 같은 이유 때문에 일부에서는 파밍에 대한 우려가 높고 대규모 피해를 예상하기도 한다.

그러나 필자는 파밍에 대한 정확한 이해와 다음과 같은 이유로 파밍이 미치는 영향이 제한적일 것으로 예측된다.

첫째, DNS의 변조가 쉽게 이뤄지기 힘들다는 점이다. ISP(Internet Service Provider)에서 운영하는 DNS 서버 및 상위계층에 위치한 DNS 서버는 중요한 인프라로 인식되어 관리되고 있기 때문이다. 그만큼 해당 DNS 서버를 위 변조하기란 쉽지 않을 것이며, 만약 공격대상이 된다 하여도 이러한 대상은 대학, 중소업체에서 운영하는 DNS 서버로 범위가 한정되어 보안이 다소 간과되기 쉬운 점을 이용할 것이다.

둘째, 대중적 방법으로 폭 넓게 사용되기 힘들다. 상위 DNS에 변조가 일어나게 되면 광범위하게 전체적인 DNS 구조에 영향을 미치기 때문에 변조 사실이 금방 알려지게 될 것이다. 큰 사회적 파장을 가져올 수 있으므로 피싱 공격자들이 과연 이러한 방법으로까지 정보를 획득하려고 할 것인가가 의문시 된다. 그러므로 트로이목마와 같은 악성코드를 이용한 클라이언트의 호스트 파일 변조 또는 DNS 설정 주소의 변경 등 제한적인 이용이 될 것이다.

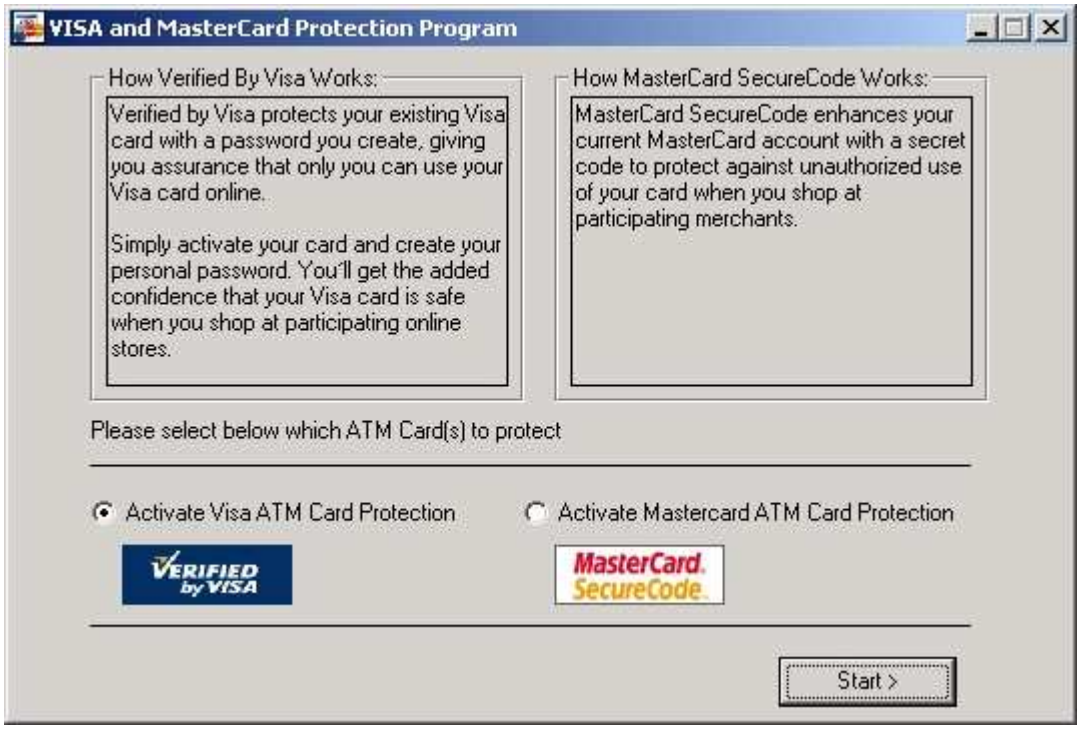
셋째, 피싱 공격자들의 투자대비수익률(ROI)을 생각해 볼 수 있다. 파밍 공격을 경제 관점 원리에서 보면 DNS 변조를 통해 얻어 낼 수 있는 가치를 생각해 보지 않을 수 없다. DNS 변조를 위해서는 공격자들에게 더욱 많은 지식을 필요로 하고 있고 이것을 구현하기 위한 시간적 비용과 기술적 노력들이 필요하게 된다. 또한 피싱 사이트의 생존기간이 평균적으로 6일 이내로 길지 않다는 점을 보면 파밍으로 통해 얻을 수 있는 가치가 제한적이게 된다.

위의 이유들을 종합해보면 파밍공격을 위해서는 기술적 지식의 필요와 어려움이 존재하고 있고 피싱 사이트들의 평균 생존기간 또한 짧기 때문에 중소 규모의 DNS 변조나 클라이언트 기반의 호스트 파일 변경 및 DNS 설정 변경과 같은 형태로 발전할 가능성이 높다. 사용자가 인지하지 못한다면 지속적인 정보수집의 가능성도 존재하지만 이것은 넓은 범위로 이용되기 보다는 제약적인 형태에서 클라이언트를 기반으로 한 파밍 공격이 이뤄질 것으로 판단된다.

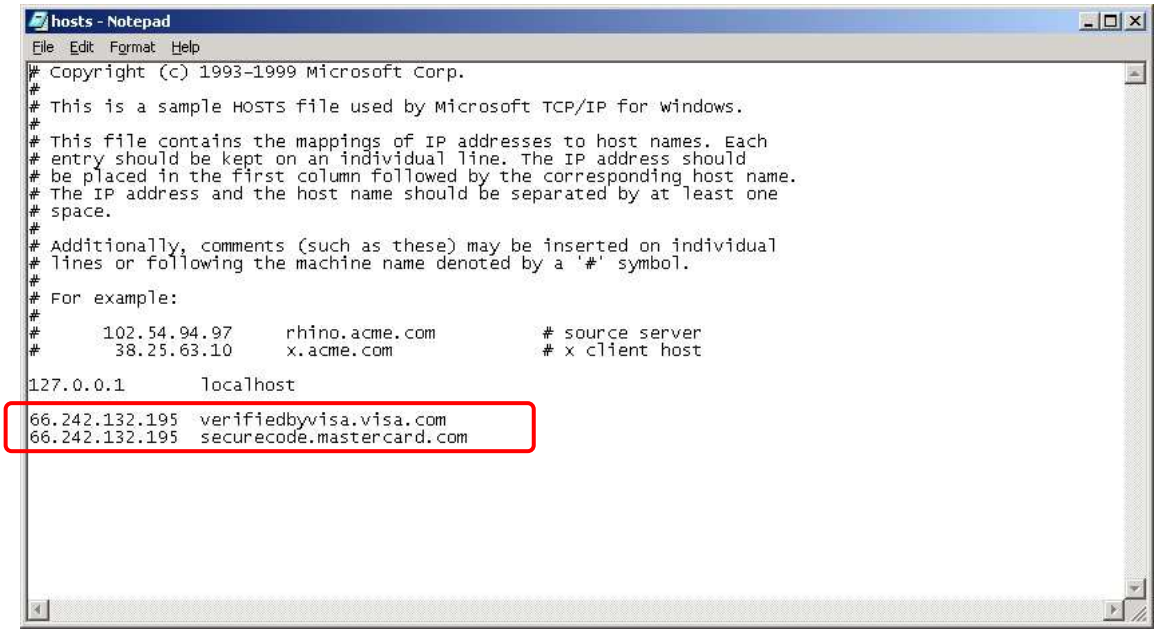
이것은 최근의 피싱 트렌드가 사용자의 입력과 같은 직접적인 행동을 요구하던 것에서 벗어나 악성코드와의 결합, 취약점 이용, 주소변경을 기반으로 하는 파밍과 같이 사용자들이 피싱공격을 인지하기 더욱 어렵도록 기술적 변화를 가져오고 있다.

실제로 최근에 발견된 트로이목마 카드넘(Win-Trojan/PWS-Cardnum.36864)은 사용자의 카드 번호 입력을 요구하는 피싱 사이트로 연결한다. 이것은 앞서 언급한 파밍 방법의 하나로 소개한 클라이언트의 호스트 파일 정보를 수정해 사용자가 더욱 믿음을 갖도록 도메인 이름을 해당 기관명의 이름으로 사용하여 접속하게 된다. 사용자 관점에서는 특정 IP로 접속

하게 되는 것이 아니라 금융기관의 도메인 주소로 접속을 하게 되므로 의심하기란 더욱 어려워 지게 된다.



[그림2] 트로이목마 카드넘 화면



[그림3] 트로이목마 카드넘의 호스트 파일 정보 수정

해당 사이트는 이미 폐쇄되어 접속할 수 없으나 앞서 예측한 것과 같이 피싱이 트로이목마

와 결합되어 발전할 가능성이 더욱 높아지리라 생각한다.

이렇게 날로 발전하고 있는 기술적 변화에 따라 피싱 뿐만 아니라 여러 보안 위협들이 증대되고 있는 만큼 사용자들의 컴퓨터 보안이 얼마나 중요해지고 있는지 보여주고 있다. 현재의 피싱은 위협으로부터 개인 사용자들을 보호하는 데에는 제품측면에서 한계가 존재하기 때문에 제한적인 역할밖에 수행할 수 없다. 그렇기 때문에 파밍과 같은 공격에 근본적인 해결은 ISP 또는 각 서비스운영업체들의 DNS 및 기타 시스템들의 안전한 운영이 필수 조건이고 개인 또한 이러한 위협으로부터 보호 받기 위하여 보안에 대한 인식의 전환이 있어야 한다.

필자는 이번 파밍이 새로운 개념이 아니라 피싱의 또 다른 공격의 하나일 뿐이라는 것으로 정의 내리고 싶다. 앞으로도 파밍과 같은 기술적 이용의 확대는 증대될 것이고 이번 파밍과 같이 위험에 대한 예측이 너무 크게 확대되지 않았으면 하는 바람으로 이 글을 마무리하고자 한다. 마지막으로 이제 보안은 제품, 서비스에 의존하는 형태에서 탈피하여 자기 스스로가 지킬 수 있어야 함을 이번 피싱과 파밍의 계기로 다시 한번 되새겨 보아야 할 것이다.