AntiVirus XP 2008 Fake Anti-Virus FAQ

질문 1. AntiVirus XP 2008은 어떤 프로그램인가요?

Antivirus 2008은 시스템에 설치될 경우 시스템을 검사하여 악성코드에 감염된 것처럼 허위로 검사결과를 사용자에게 보여주고 치료하기 위해서 결제를 유도함으로써 금전적 이득을 취하기 위한 허위 백신이다.

질문 2. AntiVirus XP 2008은 어떤 경로를 통해 유포되나요?

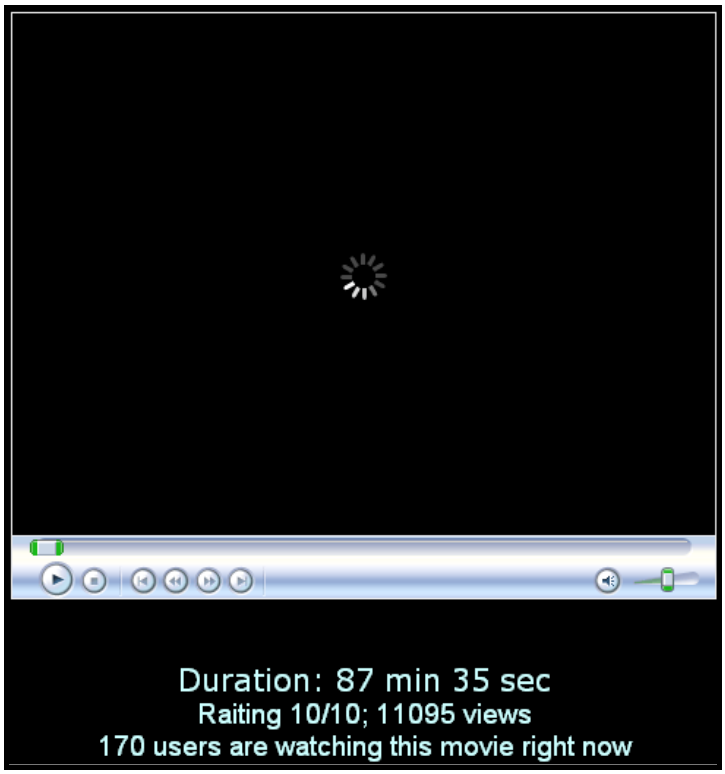
AntiVirus 2008은 아래 경우처럼 사회공학기법을 사용하여 유명 연애인(안젤리나 졸리, 브리트니 스피어스, 린제이 로한) 또는 언론사(CNN) 그리고 정치(부시) 등과 관련된 내용으로 위장하여 스팸메일의 링크 또는 첨부파일형태로 유포된다.

예1) 첨부파일형태의 경우
- 제 목 : Anjelina Jolie Free Video.
- 본 문 : 없음
- 첨부파일 : Angelina_Jolie.rar

예2) 링크형태의 경우 1
- 제 목 : Lindsay Lohan and Paris Hilton lesbian video
- 본 문 : Click Here! (http://017cb18.net******st.com/index_12.html)

예3) 링크형태의 경우 2
- 제 목 : Special video for plugins
- 본 문 : Be the first to watch it(http://017cb18.net******st.com/index_12.html)

예4) 링크형태의 경우 3
- 제 목 : Britney did it again! Really funny.
- 본 문 : Click Here!(http://www.des*******.com/index_12.html)



[그림 1. 동영상으로 위장한 AntiVirus XP 2008]

사용자가 링크를 클릭할 경우 링크된 사이트로 이동하여 메일 내용과 관련된 동영상을 재생하는 것처럼 [그림 1.]을 보여주며 동영상을 재생하기 위해서는 [그림 2]처럼 Codec을 다운로드 하도록 유도한다.

[그림 2. Codec으로 위장한 AntiVirus XP 2008]

AntiVirus XP 2008은 [그림 2]처럼 Video codec Error란 가짜 메시지 창을 출력하고 사용자로 하여금 Codec을 다운로드 하도록 유도하며 관련 웹 페이지 소스를 보면 아래와 같다.

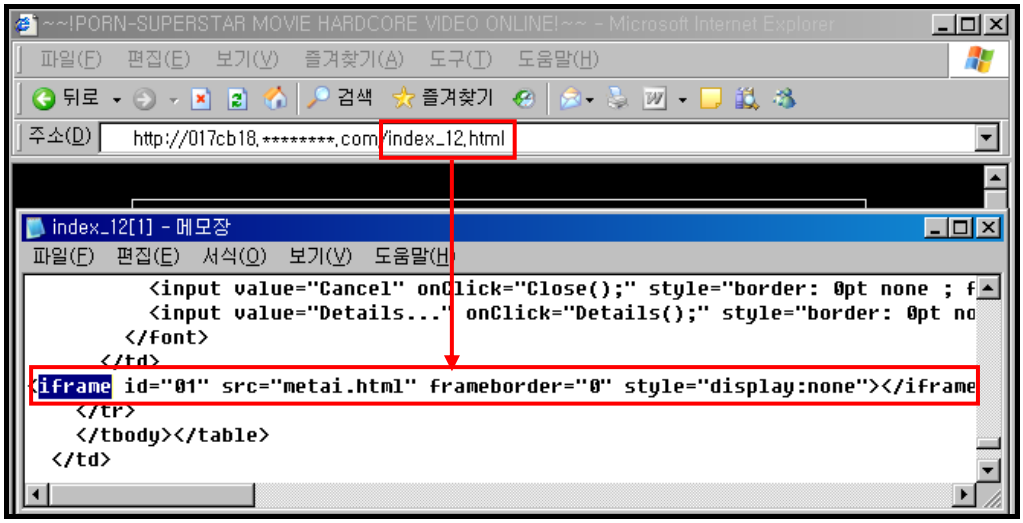
```
<font style="font-size: 11px;" color="#000000" face="Tahoma">
  To download and install ActiveX Object click <a href="install.exe" style="fo
  font-variant: normal; font-weight: normal; font-size: 11px; line-height: nor
  font-stretch: normal; color: rgb(0, 0, 0); text-decoration: underline;">Cont
  <input value="Continue" onClick="Down('iax');" style="border: 0pt none ; fon
  font-weight: bold; color: rgb(255, 255, 255); background-color: rgb(0, 156,
  type="submit">
  <input value="Cancel" onClick="Close();" style="border: 0pt none ; font-fami
  bold; color: rgb(255, 255, 255); background-color: rgb(161, 161, 161);width:
  <input value="Details..." onClick="Details();" style="border: 0pt none ; fon
  font-weight: bold; color: rgb(255, 255, 255); background-color: rgb(161, 161
  type="submit">
```

[그림 3. 다운로드 관련 웹 페이지 소스]

[그림 3]을 보면 Continue를 클릭하면 install.exe가 다운로드 되지만 Cancel를 클릭할 경우 Close()함수를 호출하여 "Click 'OK' to download and install media codec." 및 Click 'OK' to download and install media codec.라는 경고창을 계속 출력하게 된다. 또한 Details를 클릭하면 Details()함수를 호출, "Click 'OK' to download and install media codec."를 출력하고 install.exe를 다운로드 하도록 유도한다.

질문3. AntiVirus XP 2008를 다운로드 하지 않았는데도 설치되요!

AntiVirus XP 2008은 사용자가 링크로부터 파일을 다운로드 한 후 실행해야지만 설치되는 것은 아니며 이는 사용자를 속이기 위한 하나의 위장수단이다. AntiVirus XP 2008가 유포되는 사이트의 웹 페이지 소스를 보면 Exploit을 통해서 시스템에 AntiVirus XP 2008이 다운로드 및 설치될 수 있도록 iframe이 삽입되어 있음을 알 수가 있다.



[그림 4. 삽입된 iframe]

* AntiVirus XP 2008가 유포 시 자주 사용하는 취약성을 살펴 보면 다음과 같다.

▶ COM 개체(Msdds.dll)로 인한 Internet Explorer의 예상치 못한 종료
EC444CB6-3E7E-4865-B1C3-0DE72EF39B3F
http://www.microsoft.com/korea/technet/security/Bulletin/MS05-052.mspx

▶ MDAC(Microsoft Data Access Components) 기능의 취약점으로 인한 원격 코드 실행 문제점
BD96C556-65A3-11D0-983A-00C04FC29E36
http://www.microsoft.com/korea/technet/security/bulletin/MS06-014.mspx

▶ Microsoft Access Snapshot Viewer에서 사용하는 ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점
F0E42D50-368C-11D0-AD81-00A0C90DC8D9
http://www.microsoft.com/korea/technet/security/bulletin/MS08-041.mspx

▶ Online Media Technologies NCTsoft NCTAudioFile2 ActiveX buffer overflow
77829F14-D911-40FF-A2F0-D11DB8D6D0BC
http://www.kb.cert.org/vuls/id/292713

▶ RealNetworks RealPlayer ActiveX controls property heap memory corruption
2F542A2E-EDC9-4BF7-8CB1-87C9919F7F93
http://www.kb.cert.org/vuls/id/831457

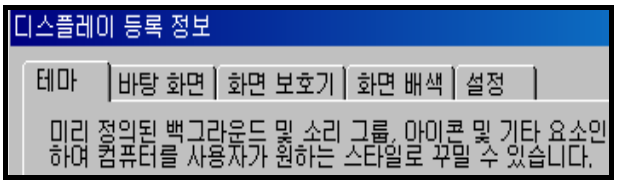
위에서 언급된 취약성 외에도 다양한 취약성을 사용할 수 있으므로 자신이 사용하는 OS 및 소프트웨어를 주기적으로 점검 및 보안패치를 적용해 주는 것이 좋다.

질문4. AntiVirus XP 2008가 설치되면 시스템에 어떤 증상이 발생하나요?
AntiVirus XP 2008가 설치되었을 경우 대표적인 증상을 정리해 보면 다음과 같다.

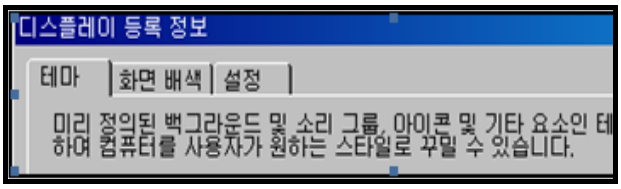
(4-1) 바탕화면이 변경됐어요!
AntiVirus XP 2008은 자신이 생성한 그림파일을 사용하여 아래 그림처럼 시스템의 바탕화면으로 설정한다.
(참고로 그림파일은 가변적이다.)

[그림 5. 변경된 바탕화면]

또한 사용자가 바탕화면을 변경할 수 없도록 레지스트리를 변경하여 [그림 7]에서 보는 것처럼 바탕화면 관련메뉴를 안보이게 한다.



[그림 6. AntiVirus XP 2008 감염 전]



[그림 7 AntiVirus XP 2008 감염 후]

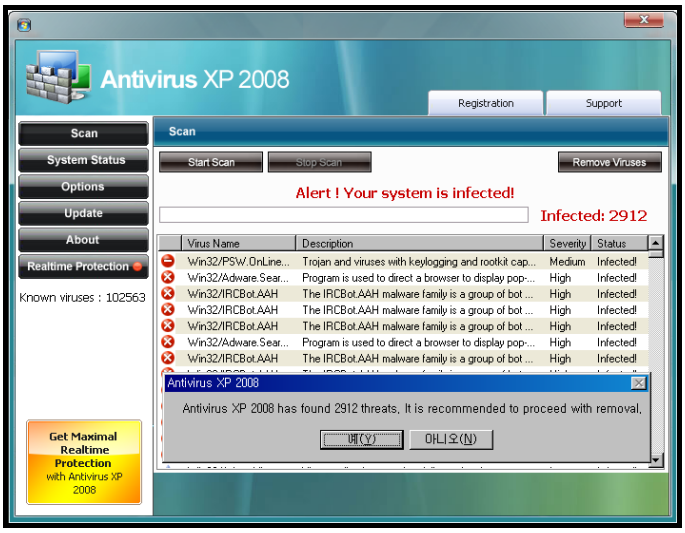
SpyZero에서는 AntiVirus XP 2008관련 파일을 진단 및 치료할 수 있는 경우에 한하여 변경된 레지스트리 값을 복원시켜 준다. 만약 사용자가 수동으로 복구를 하고자 할 경우 아래 내용을 참조하면 된다.

*** 바탕화면 메뉴관련 레지스트리 복구방법 :**

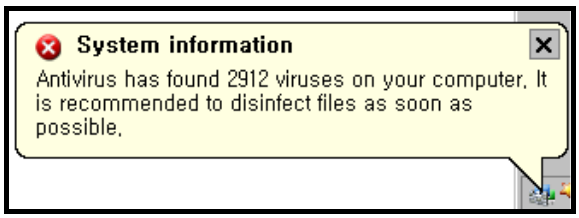
시작 -> 실행 -> regedit.exe -> 레지스트리 편집기 실행 -> 아래 경로로 이동한 후 해당 값들을 선택한 후 마우스 오른쪽 버튼을 클릭하여 삭제하거나 아래와 같이 수정하면 [그림 6]처럼 복원할 수 있다

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
NoDispBackgroundPage="0x00000001" 에서 "0x00000000"로 수정
NoDispScrSavPage="0x00000001" 에서 "0x00000000"로 수정

(4-2) 주기적으로 허위 검사 결과 및 팝업이 출력되요!~



[그림 8. 허위 검사 화면]

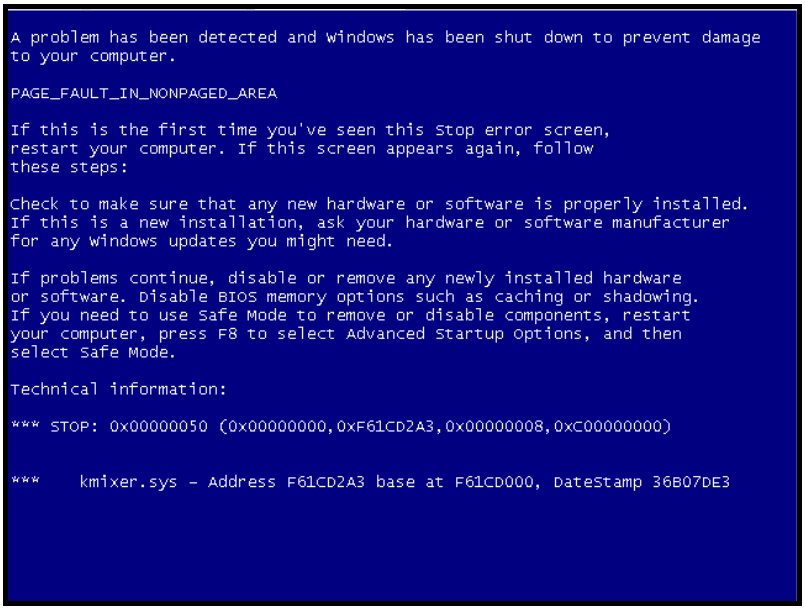


[그림 9. 시스템 트레이 팝업]

AntiVirus XP 2008의 대표적인 증상으로 주기적으로 검사결과 및 시스템 트레이에 팝업을 보여줌으로써 사용자에게 불안감 조성 및 치료를 위한 결제를 유도한다.

(4-3) 화면보호기 파일을 이용한 Joke Blue Screen 발생해요!~

AntiVirus XP 2008은 정상 화면보호기 파일을 사용하여 일정시간이 지나면 아래처럼 Joke Blue Screen 및 부팅화면을 반복한다.



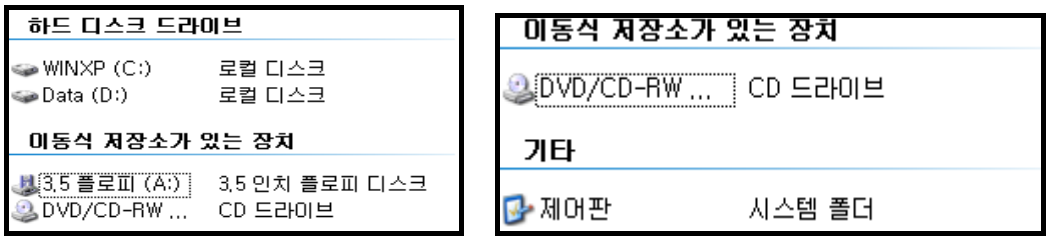
[그림 10. 가짜 블루 스크린]

[그림 11. 가짜 부팅 화면]

[그림 10]에서 보면 Blue Screen원인이 되는 파일은 임의로 변경되며 실제 해당 파일에 문제가 있는 것은 아니지만 위 두 그림만 놓고 보면 사용자 입장에서는 마치 자신의 시스템에 문제가 있는 것으로 충분히 오해할 수 있는 소지가 있다.

(4-4) 내 컴퓨터에 들어가 보면 드라이브가 안 보여요!~

현재 AntiVirus XP 2008은 수많은 변종이 존재하는데 일부 변종에서는 드라이브의 속성이 Fixed(보통, HDD)일 경우 사용자가 볼 수 없도록 숨기는 경우도 있다.



[그림 12. 변경 전과 후]

*** 드라이브 속성 복구방법 :**

시작 -> 실행 -> gpedit.msc를 입력한 후 확인 -> 그룹 정책편집기 실행 -> 사용자 구성 -> 관리 템플릿 -> Windows 탐색기 -> [내 컴퓨터]에 있는 지정된 드라이브 숨기기 더블클릭 -> 사용 안 함(D) -> 적용 -> 구성되지 않음(C) -> 적용

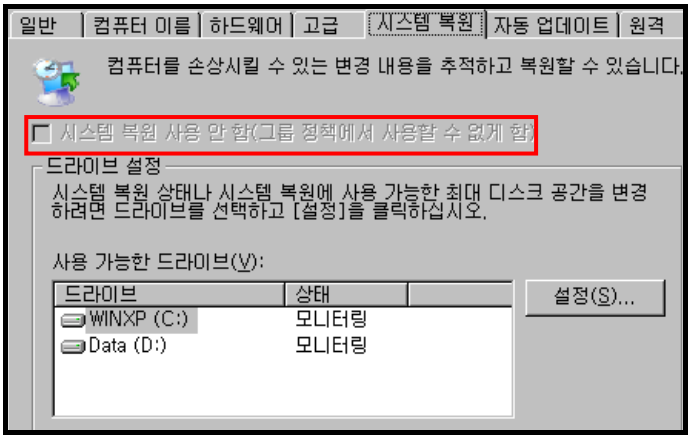
(4-5) 시스템 복원해도 AntiVirus XP 2008이 재 감염 되요!

AntiVirus XP 2008은 %Temp%폴더에 VBS(Visual Basic Script)로 작성된 스크립트를 생성 및 실행하여 시스템 복원이 사용중이라면 복원기능을 비활성화하여 기존의 복원시점을 삭제한 후 재 활성화시킨 후 복원시점을 AntiVirus XP 2008이 설치된 시점으로 설정한다.

이렇게 되면 사용자가 시스템 복원기능을 사용하여 복구하더라도 계속 재 감염되는 문제가 발생하므로 일시적으로 시스템 복원기능을 해제하여 복원시점을 초기화시킨 후 백신으로 치료하고 복원시점을 재설정해야 한다.

(4-6) 시스템 복원기능을 사용할 수 없어요!

AntiVirus XP 2008의 일부 변종은 사용자가 시스템 복원기능을 제어할 수 없도록 아래 그림처럼 그룹정책을 조작하여 시스템 복원시점을 초기화 할 수 없도록 비활성화시킨다.



[그림 13]시스템 복원 시점 초기화 불가

*** [시스템 복원 사용 안 함] 옵션이 비활성화 된 경우 복구방법 :**

시작 -> 실행 -> gpedit.msc를 입력한 후 확인 -> 그룹 정책편집기 실행 -> 컴퓨터 구성 -> 관리 템플릿 -> 시스템 -> 시스템 복구 -> 구성을 사용하지 않음 더블클릭 -> 사용 안 함(D) -> 적용 -> 구성되지 않음(C) -> 적용

만약 그룹 정책편집기 실행이 불가능하다면 아래 방법을 사용하여 시스템 복원 모니터링을 사용 안 함으로 설정할 수 있다.

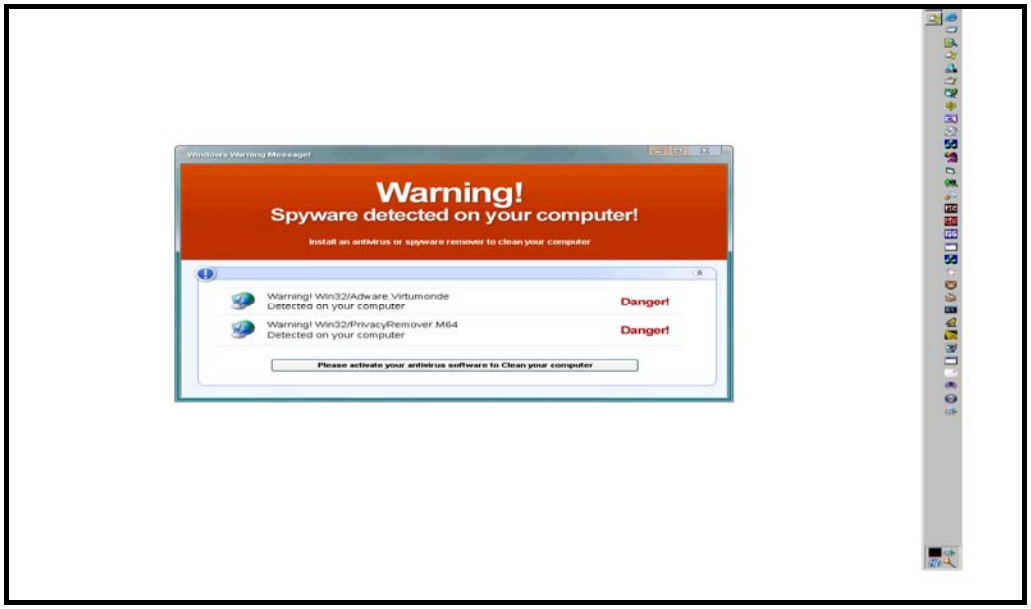
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\
DisableSR="1"로 설정

(4-7) 바탕화면 아이콘이 사라졌어요!~

AntiVirus XP 2008의 일부 변종은 바탕화면의 아이콘 표시기능을 해제하여 안 보이도록 한다.

*** 바탕화면 아이콘 복구방법 :**

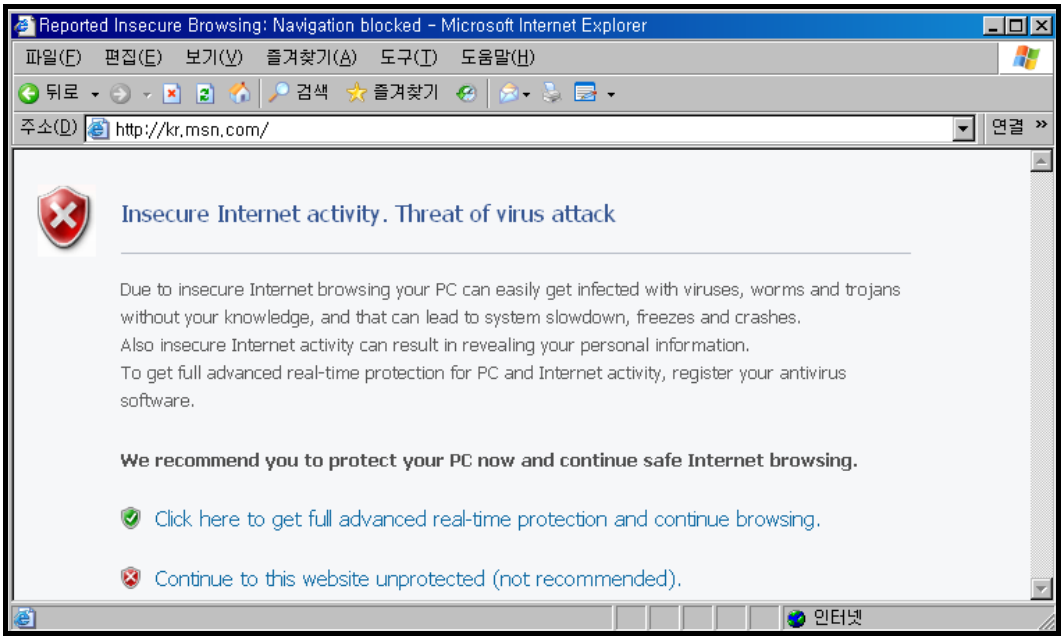
바탕화면에서 마우스 오른쪽 버튼 클릭 -> 아이콘 정렬 순서(I) -> 바탕화면 아이콘 표시(D)를 클릭하면 사라졌던 바탕화면 아이콘을 복구할 수 있다.



[그림 14. 사라진 바탕화면 아이콘]

(4-8) 특정 사이트에 접속하면 AntiVirus XP 2008사이트로 이동해요!~

사용자가 특정 사이트에 접속할 경우 간헐적으로 해당 사이트를 차단하고 아래 그림처럼 경고 메시지를 출력한다.

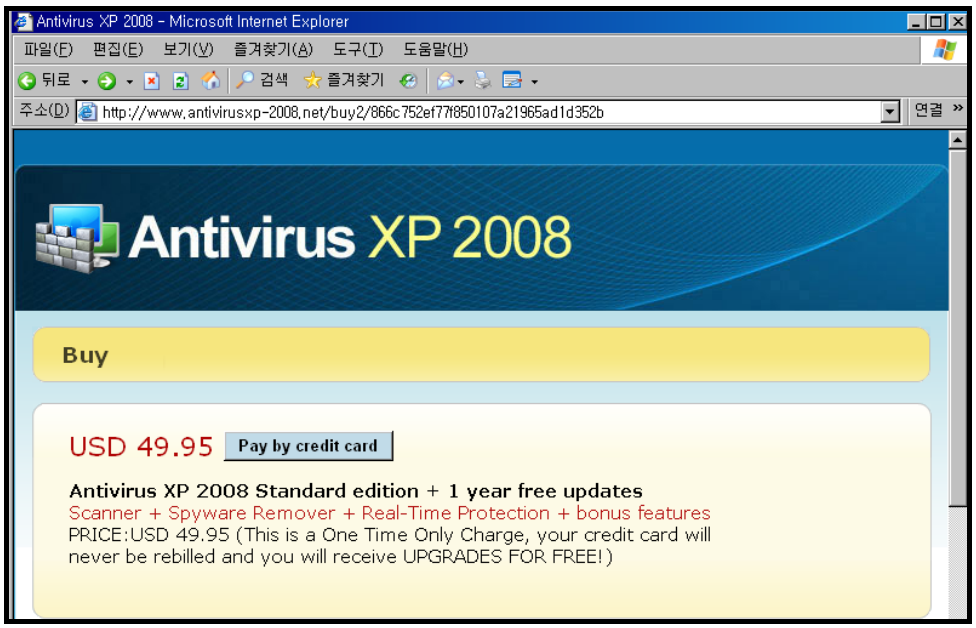


[그림 15. 특정 사이트 차단]

*** 사이트 차단 목록**

mac.com/nytimes.com/download.com/gamespot.com/partypoker.com/mediafire.com/geocities.com/ 56.com/ about.com/deviantart.com/yourfilehost.com/apple.com/adobe.com/imagevenue.com/livejournal.com/ go.com mininova.com/redtube.com/craigslist.com/tinyurl.com/adultfriendfinder.com/skyrock.com/friendster.com flickr.com/wordpress.com/youporn.com/imdb.com/amazon.com/photobucket.com/aol.com/hi5.com/ebay.com/rapid share.com/orkut.com/blogger.com/facebook.com/wikipedia.org/microsoft.com/myspace.com/msn.com/live.com/ya hoo.com/google.com/ megaupload.com

[그림 15]에서 보이는 두 링크를 클릭할 경우 [그림 16]처럼 AntiVirus XP 2008 구매사이트로 접속을 유도한다.



[그림 16. AntiVirus XP 2008 구매 사이트]