대량의 스팸메일을 이용한 허위백신 유포사례 분석

1. 개요

최근 악성코드 전파를 목적으로 발송되는 스팸메일이 지속적으로 증가하고 있다. 발견된 스팸메일들은 해외 유명 연예인과 관련된 내용이나 최근 사회적으로 이슈가 되고 있는 내용과 함께 추가적인 정보를 제공하는 링크를 포함하고 있다. 스팸메일에 포함된 내용은 대부분 허위 사실로 메일 수신자들이 관련 링크를 클릭하도록 유도하고 있다. 해당 링크를 클릭할 경우, 악성코드가 직접 다운로드 되거나 악성코드를 유포하는 사이트로 연결된다. 이러한 악성코드 유포 방법을 사회공학적 기법이라 한다.

최근 발송된 스팸메일을 통해 다운로드된 악성코드들은 직접 실행되지는 않으나 스팸메일과 관련된 내용의 동영상 파일이나 코덱으로 위장하여 사용자들의 실행을 유도한다. 스패머들은 스팸메일에 포함된 내용이나 악성코드 및 악성코드 유포지를 계속 변경하여, 스팸필터를 이용한 스팸메일 차단이나 백신을 이용한 악성코드 진단/치료를 어렵게 하고 있다.

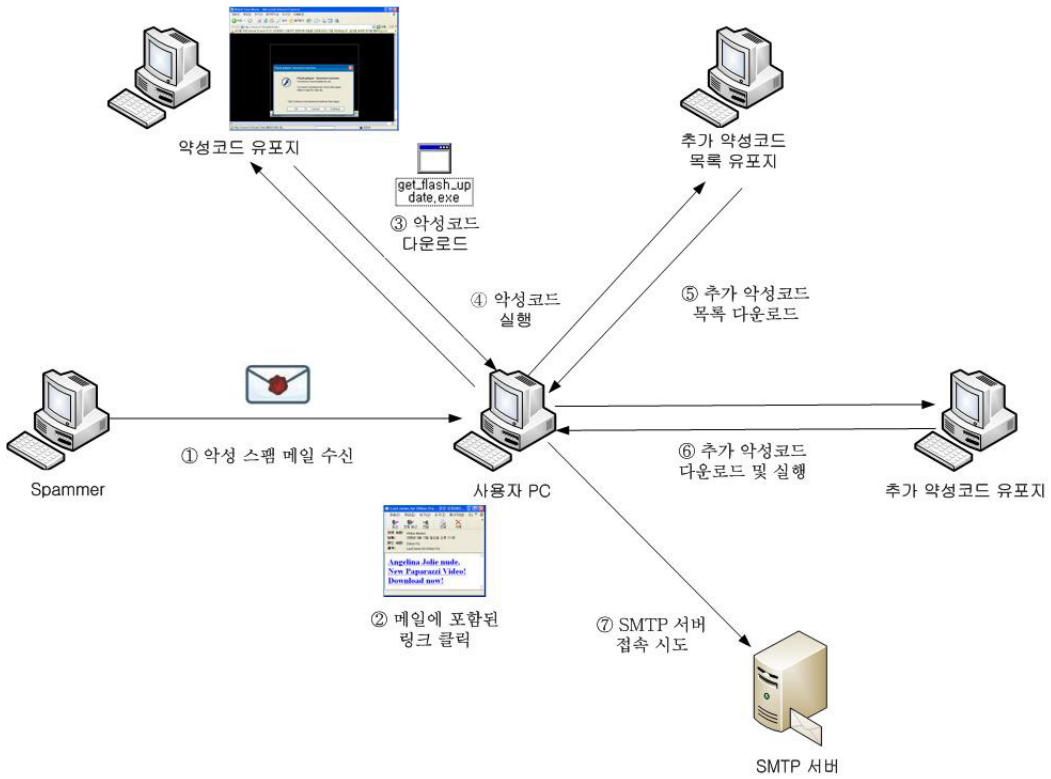
다운로드된 악성코드들은 다양하나 주로 다운로더들로서 직접적인 악성행위는 수행하지 않지만 추가 악성코드 유포지로부터 또 다른 악성코드를 다운로드하여 감염 PC에 설치한다. 설치된 추가 악성코드들은 감염 PC의 바탕화면과 화면보호기를 변경하고 허위백신을 설치하는 그레이웨어 (Grayware)로서 사용자의 불안 심리를 조장하여 금융 결제를 유도한다.

이메일 사용자들은 신뢰할 수 없는 이메일이나 사이트를 통해 의심이 가는 파일을 다운로드하거나 실행하지 않도록 주의해야 한다. 또한, 운영체제와 백신프로그램의 업데이트 서비스를 통하여 컴퓨터의 보안 업데이트를 최신 상태로 유지하고 백신프로그램의 실시간 감시기능을 활성화하여 악성코드에 감염되지 않도록 예방하는 것이 중요하다.

2. 악성코드 유포사례 상세

가. 악성코드 유포 개요도

이번 악성코드 유포사례에 대한 전체적인 개요는 아래 그림과 같이 악성코드 유포 서버, 추가 악성코드 목록 유포 서버, 추가 악성코드 유포 서버 그리고 SMTP 서버 및 감염 PC로 이루어진다.



(그림) 악성코드 유포 개요도

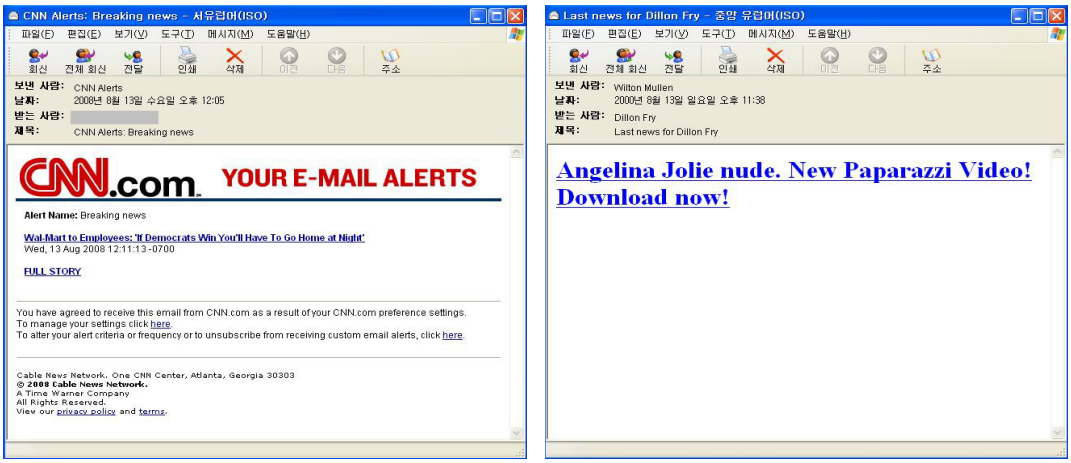
나. 유포사례 대응

이번 대량의 스팸메일을 이용한 악성코드 유포사례는 8월 5일 국외 보안 사이트에서 최초로 관련 내용이 공개되었으며, 인터넷침해사고대응지원센터에서도 관련 악성코드 입수 및 유포사이트 차단 등을 통하여 피해를 최소화하였다.

다. 스팸메일 유형 분석

○ 스팸메일 제목 및 내용

스팸메일 제목에는 'CNN 속보', '베이징 올림픽', '세계 3차대전 시작' 등 인터넷 사용자들을 현혹하는 문구가 포함되어 있으며 메일 내용에는 해외연예인, 동영상, 플레시 플레이어, 인터넷 익스플로러(IE7) 최신버전 등을 언급하여 메일 수신자들로 하여금 메일에 포함된 링크를 클릭하도록 유도함으로써 악성코드를 감염시킨다.



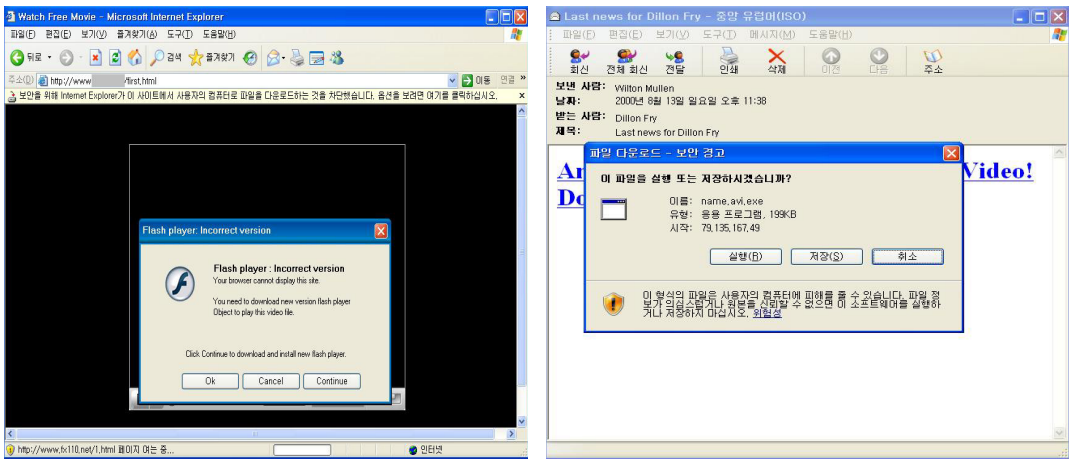
(그림) 스팸메일 제목 및 내용

이러한 스팸메일의 제목은 메일마다 다르고 계속 변경되나 주로 다음과 같다.

주제	메일제목
CNN	CNN Alerts: My Custom Alert
	CNN.com Daily Top 10
	CNN Alerts: Breaking news
	CNN Daily Top 10
Angelina Jolie	Angelina Jolie Free Video
	Angelina Jolie's Free Video
	Angelina Jolie nude movie
	Angelina naked video
	Angelina Jolie gives birth to triplets
	Angelina Jolie dies in miscarriage
McCain & Obama	McCain supports idea that Obama is muslim
	Obama admits extra-marital affair
World War	Bush unveils Iran invasion plan
	US Army invades southern Iran
Olympics	Beijing Olympics cancelled
etc	We congratulate!

o 메일에 첨부된 악성코드 및 악성코드 유포 사이트 링크

메일 수신자는 스팸메일에 첨부된 링크를 클릭함으로써 악성코드가 직접 다운로드 되거나 악성코드를 유포하는 사이트로 연결된다.



(그림) 유포사이트를 이용하는 경우(좌)와 직접 다운로드 되는 경우(우)

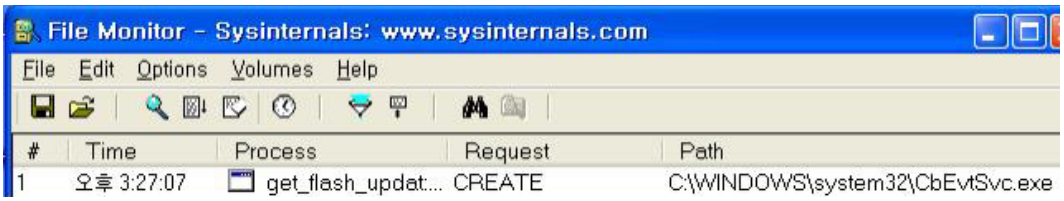
이러한 악성코드나 악성코드 유포지 주소가 메일마다 다르나 메일 본문과 관련된 파일이나 사이트로 위장하여 악성코드의 다운로드 및 실행을 유도한다. 악성코드 유포지를 통하여 악성코드가 다운로드 되는 경우에는 사이트에서 제공하는 동영상을 감상하기 위해 필요한 코덱의 설치 파일로 악성코드를 위장하고 있다. 다운로드 되는 악성코드들은 주로 다음과 같은 파일명을 가지고 있다.

xvideo.avi.exe, update.exe, Paris-nude-video.avi.exe, video.avi.exe, flash.exe, video54582.exe, video9865565.exe, video-anjelina.avi.exe, windows_media.exe, video-nude-anjelia.avi.exe, video435ki.exe, flashupdate.exe, shok_video.exe, flashcodecinstall_13_31.exe, watch.exe, codecinst.exe, video1.exe, video.exe, hot_video.exe, video_film.exe, xxx.exe, videousa.exe, video6.exe, video12.exe, watchmovie.mpg.exe, msvideoc.exe

라. 악성코드 분석

o 악성코드 감염 절차

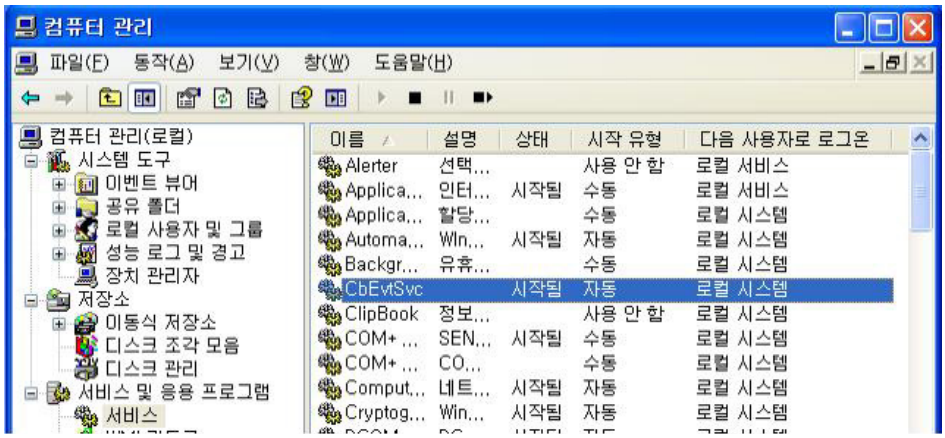
① 악성코드 유포 서버로부터 다운로드된 get_flash_update.exe를 실행시키면 C:\WINDOWS\system32\CbEvtSvc.exe의 경로로 자기 복제를 하고 실행시킴으로써 악성행위를 시작한다.



(그림) 악성코드 복사

② CbEvtSvc.exe를 다음과 같은 서비스로 등록하여 시스템 시작 시 자동 실행되도록 한다.

```
Name: CbEvtSvc
Display Name: CbEvtSvc
Description: (없음)
Module: C:\WINDOWS\system32\CbEvtSvc.exe
```



(그림) 서비스 등록

③ CbEvtSvc.exe는 우선 추가 악성코드 목록 유포지인 https://66.199.xxx.xxx에 접속하여 추가 악성코드 목록인 /ldrctl/ldrtcl.php를 받아와 이에 포함되어 있는 주소를 통해 추가 악성코드들의 위치를 파악한다. 추가 악성코드 목록 유포지 주소 및 목록 파일명은 CbEvtSvc.exe에 하드코딩 되어있다.

④ CbEvtSvc.exe는 추가 악성코드 목록에 포함되어 있는 추가 악성코드들을 다운로드하여 실행시킨다. 추가 다운로드 및 실행된 악성코드들은 다음과 같다.

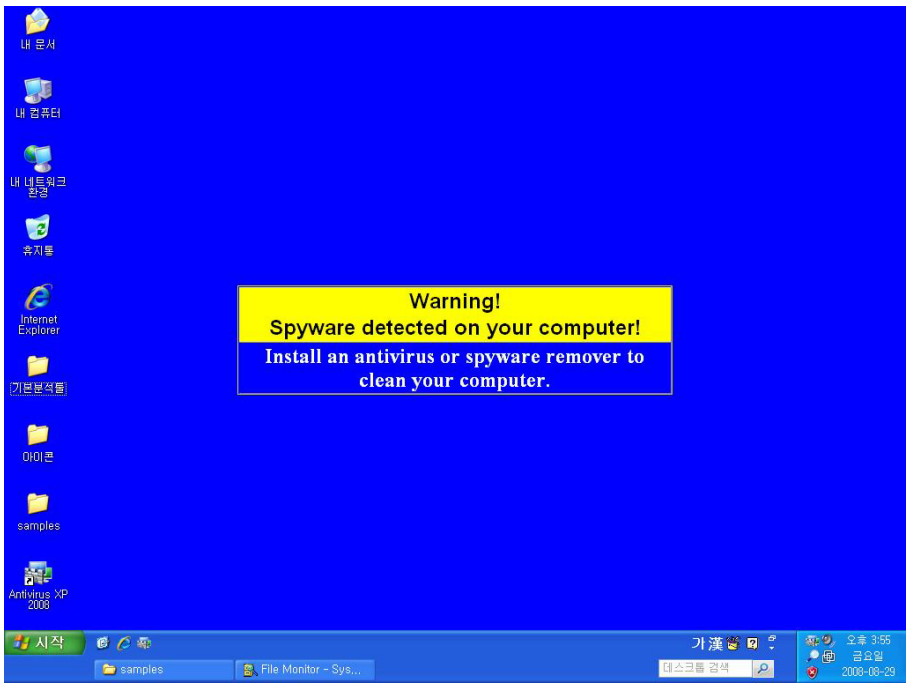
```
http://78.109.xxx.xxx/04scan.exe
http://78.109.xxx.xxx/install.exe
```

⑤ 추가로 다운로드 된 04scan.exe가 실행되면 PC의 바탕화면, 화면보호기 등을 변경하고 허위백신을 설치한다.

⑥ 추가로 다운로드 된 install.exe가 실행되면 google, yahoo, aol, microsoft, frontbridge 등의 SMTP 서버로 접속을 시도하고 그 결과를 특정 사이트로 전달한다.

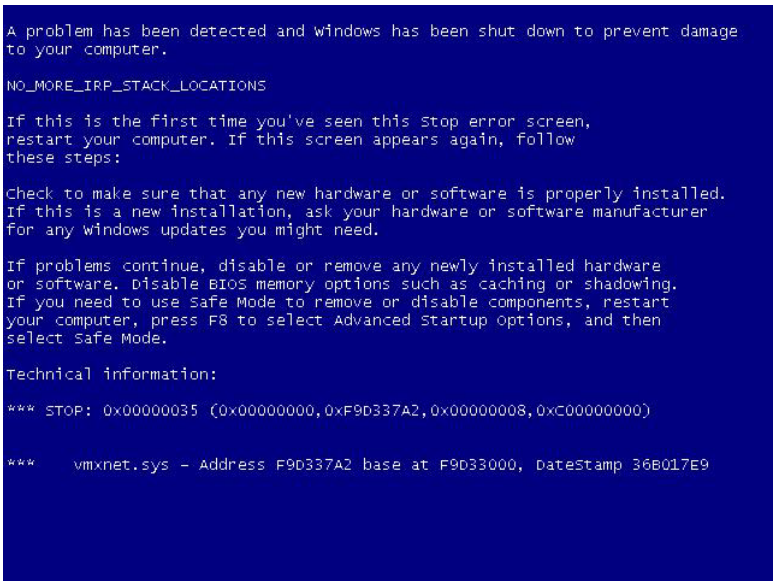
o 악성코드에 감염된 PC에서 발생하는 피해 증상

- 악성코드가 실행되면 우선 바탕화면을 다음과 같이 변경하여 PC가 스파이웨어에 감염되었으니 백신을 설치해야 한다고 사용자에게 경고한다.



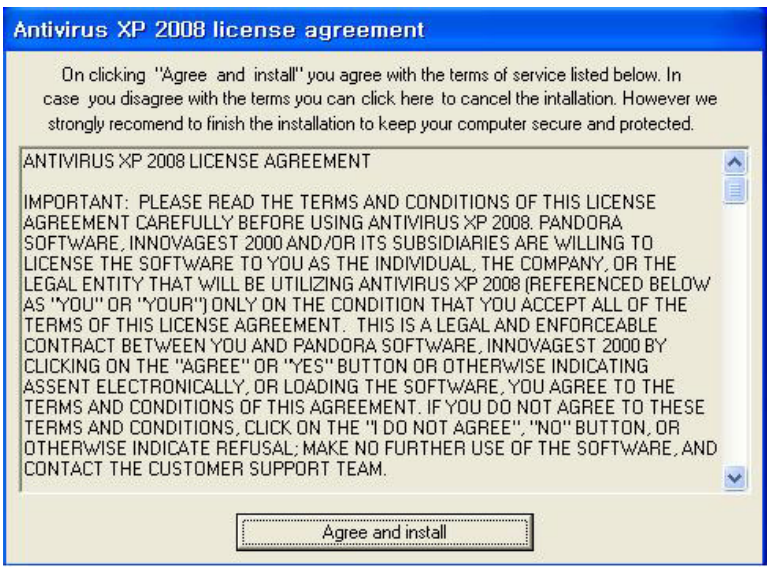
(그림) 바탕화면 변경

- 또한, 다음과 같은 윈도우즈 오류 화면으로 화면보호기를 변경하여 실제로 사용자 PC에 악성코드가 감염되어 있는 것처럼 보이도록 한다.



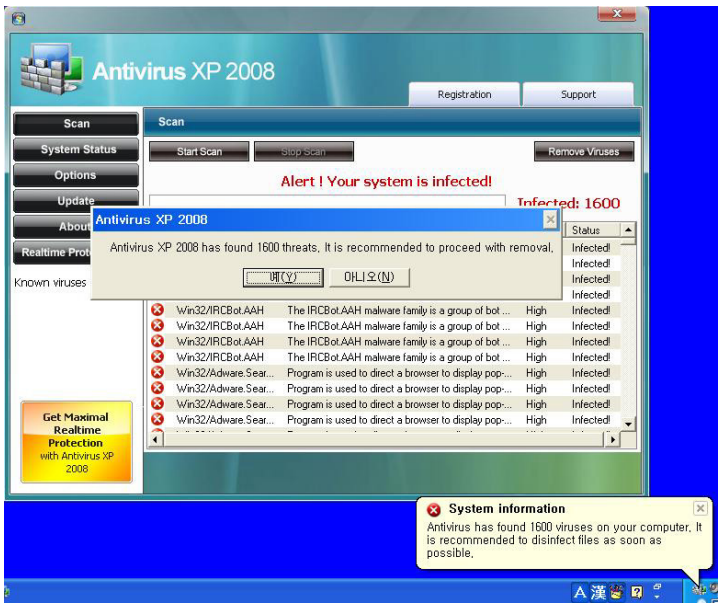
(그림) 화면보호기 변경

- 이와 같은 악성행위들은 사용자로 하여금 다음과 같이 "Antivirus XP 2008"이라는 허위백신을 설치하도록 유도하기 위함이다.



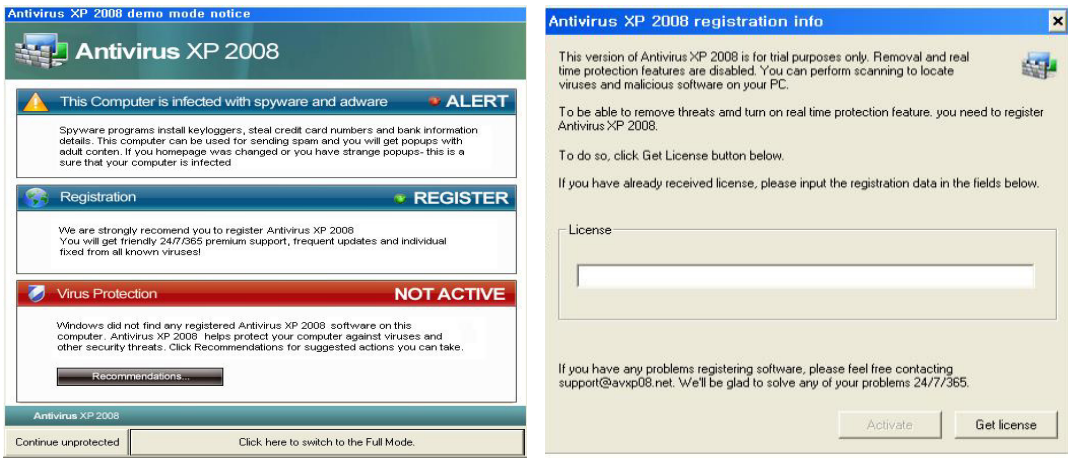
(그림) 허위백신 설치 동의 화면

- 악성코드에 의해 실행된 설치 프로그램이 사용자로 하여금 허위백신의 설치 동의를 얻고는 있으나 사용자가 설치를 거부할 수는 없도록 만들어 허위백신을 강제로 설치하도록 하고 있다. 설치된 허위백신은 사용자 PC를 진단한 뒤, 다량의 악성코드가 감염되어 있다면서 치료할 것을 권유하고 있다.



(그림) 허위백신의 허위진단 결과

- 악성코드 치료를 위해 “예(Y)” 버튼을 누르면 다음과 같이 등록되지 않은 제품이니 치료를 위해서는 라이센스 키를 구입하라고 한다. 실제, 허위백신에서 진단한 악성코드들은 사용자 PC에 존재하지 않으며 사용자가 허위백신을 구입하도록 유도하기 위해 제공한 거짓 정보이다.

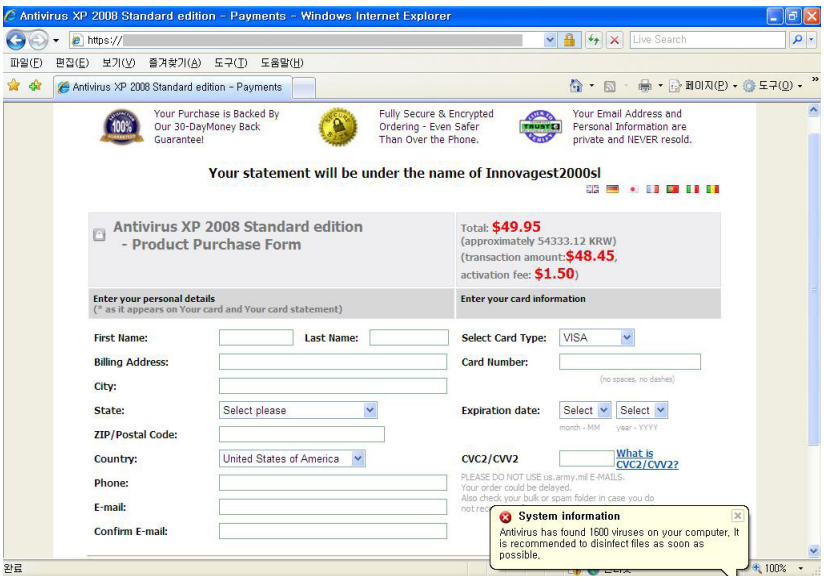


(그림) 허위백신 등록 화면

- 제품 등록을 위해 하단에 위치한 "Click here to switch to the Full Mode." 버튼이나 "Get license" 버튼을 누를 경우, 다음과 같은 라이센스 구입 사이트로 연결된다.

(그림) 허위백신 구매 사이트

- 라이센스 구입을 위해 "Pay by creadit card" 버튼을 눌렀을 경우, 다음과 같은 신용카드 결제 사이트가 열린다. 해당 결제 사이트는 사용자가 개인정보 및 신용카드 정보를 입력하고 "Process transaction" 버튼을 누르면 결제가 진행되도록 되어 있다. 해당 결제 사이트는 피싱 사이트가 아닌 실제로 신용카드 결제가 이루어지는 사이트로서 사용자들이 결제를 진행할 경우에는 금전적인 피해를 입을 위험성이 있다.



(그림) 허위백신 결제 사이트

이처럼 악성코드 유포자는 스팸메일과 악성코드를 이용하여 사용자 PC에 허위백신을 설치하고 이를 통하여 잘못된 진단 결과를 사용자에게 제공하는 방식으로, 치료를 위한 사용자 결재를 유도하고 있다. 사용자는 금전적인 피해를 예방하기 위하여 인터넷 상에서 이와 동일하거나 유사한 방식으로 금융 결제를 요구하는 상황을 접하게 될 경우 각별히 주의해야 한다.

마. 치료 방법

① 부팅 시 F8을 눌러 안전모드를 선택한다.

② 아래의 폴더와 파일들이 존재하면 삭제한다. (*은 임의의 숫자 혹은 문자)

- C:\WINDOWS\system32\CbEvtSvc.exe
- C:\WINDOWS\system32\lphc***j0e***.exe
- C:\WINDOWS\system32\pphc***j0e***.exe
- C:\WINDOWS\system32\phc***j0e***.bmp
- C:\WINDOWS\system32\blphc***j0e***.scr
- C:\WINDOWS\system32\drivers\54c70b2e.sys
- C:\WINDOWS\qegbdmwf.dll
- C:\WINDOWS\pntqkflv.dll
- C:\Program Files\rhc***j0e***
- C:\Program Files\rhc***j0e***\database.dat
- C:\Program Files\rhc***j0e***\license.txt
- C:\Program Files\rhc***j0e***\MFC71.dll
- C:\Program Files\rhc***j0e***\MFC71ENU.DLL
- C:\Program Files\rhc***j0e***\msvcp71.dll
- C:\Program Files\rhc***j0e***\msvcr71.dll
- C:\Program Files\rhc***j0e***\rhc***j0e***.exe
- C:\Program Files\rhc***j0e***\rhc***j0e***.exe.local
- C:\Program Files\rhc***j0e***\rhc***j0e***Skin.dll
- C:\Program Files\rhc***j0e***\Uninstall.exe
- C:\Documents and Settings\All Users\바탕 화면\Antivirus XP 2008.lnk
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008.lnk
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008\Antivirus XP 2008.lnk
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008\How to Register Antivirus XP 2008.lnk
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008\License Agreement.lnk
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008\Register Antivirus XP 2008.lnk
- C:\Documents and Settings\All Users\시작 메뉴\프로그램\Antivirus XP 2008\Uninstall.lnk
- %UserProfile%\Application Data\Microsoft\Internet Explorer\Quick Launch\Antivirus XP 2008.lnk
- %UserProfile%\Application Data\rhc***j0e***
- %UserProfile%\Application Data\rhc***j0e***\Quarantine
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun\HKCU
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun\HKCU\RunOnce
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun\HKLM
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun\HKLM\RunOnce
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun\StartMenuAllUsers
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Autorun\StartMenuCurrentUser
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\BrowserObjects
- %UserProfile%\Application Data\rhc***j0e***\Quarantine\Packages

③ “시작” ? “실행” 에서 regedit를 입력하고 확인 버튼을 누른다.

④ 아래의 레지스트리 항목들이 존재하면 삭제한다. (*은 임의의 숫자 혹은 문자)

- HKEY_CURRENT_USER\Control Panel\Desktop\SCRNSAVE.EXE
- HKEY_CURRENT_USER\Control Panel\Desktop\ConvertedWallpaper
- HKEY_CURRENT_USER\Control Panel\Desktop\OriginalWallpaper
- HKEY_CURRENT_USER\Control Panel\Desktop\Wallpaper
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispBackgroundPage
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoDispScrSavPage
- HKEY_CURRENT_USER\Software\Sysinternals\Bluescreen Screen Saver
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CbEvtSvc
- HKEY_LOCAL_MACHINE\SOFTWARE\rhc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\rhc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\rhc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\lphc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pphc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SMrhc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\rhc***j0e***
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform\AntivirXP08

⑤ 재부팅한다.

바. 예방 방법

우선, 이메일 사용자들은 신뢰할 수 없는 이메일이나 첨부된 링크를 통해 접속한 사이트의 문구에 현혹되어 의심이 가는 파일을 다운로드하거나 실행하지 않도록 주의해야 한다.

또한, 운영체제와 백신프로그램의 업데이트 서비스를 사용하여 컴퓨터의 보안 업데이트를 최신 상태로 유지하고 백신프로그램의 실시간 감시기능을 활성화하여 악성코드에 감염되지 않도록 예방한다.

3. 결론

최근 대량 발송된 스팸메일들은 해외 유명 연예인과 관련된 내용이나 최근 사회적으로 이슈가 되고 있는 내용을 포함하여 메일 수신자로 하여금 악성코드를 다운로드하도록 유도하고 있다. 다운로드 된 악성코드나 악성코드 유포지의 주소는 다양하나 대부분의 악성코드들이 사용자 PC에 감염된 후에 “Antivirus XP 2008“이라는 허위백신을 설치하고 있다. 감염된 악성코드는 설치한 허위백신을 통해 잘못된 진단 결과를 제공함은 물론, 감염 PC의 바탕화면과 화면보호기까지 변경함으로써 적극적으로 사용자의 허위백신 구입을 유도하고 있다.

이와 같은 스팸메일로 인한 피해를 예방하기 위해서는 이메일 사용자들은 신뢰할 수 없는 이메일의 내용이나 관련 링크를 통해 접속한 사이트의 문구에 현혹되어 의심이 가는 파일을 다운로드하거나 실행하지 않도록 주의해야 한다. 또한, 악성코드의 감염을 막기 위해서는 운영체제와 백신프로그램의 업데이트 서비스를 사용하여 컴퓨터의 보안 업데이트를 최신 상태로 유지하고 백신프로그램의 실시간 감시기능을 활성화하여야 한다. 마지막으로, 신뢰할 수 없는 사이트를 통하여 개인 정보나 신용카드 정보를 제공하지 않도록 주의함으로써 금전적인 피해를 막도록 한다.