Maxoverpro Security Lab.

Spyware.VB.20480 분석과 치료

By Maxoverpro[Max](장상근)

maxoverpro@paran.com

http://www.maxoverpro.org

이 문서는 Spyware.VB.20480 이란 악성코드의 분석과 치료에 대한 내용을 담은 문서 이다.

1. 악성코드의 행동 패턴 분석.

이 악성코드는 **ctfmon.exe** 라는 파일로 원래 **ctfmon.exe**는 **MS-Office**에서 사용자 입력을 담당하는 프로세스로 떠 있는 정상 프로세스이다. 하지만 이 악성코드는 똑같이 **ctfmon.exe**이란 파일명으로 **20,480 Byte**의 크기와 **MD5(74DBD545CF6DC5D006325CC3E4658A12)**를 가지고 있으며 아래와 같은 행동 패턴을 가지고 있다.

① 시작 프로그램에 **ctfmon.exe**을 추가.

② 각 디스크 드라이브에 시스템 파일로 **\Recycled**이란 가짜 휴지통 폴더를 생성하고 폴더 내부에는 숨김 속성으로 해서 **INFO2 , desktop.ini, ctfmon.exe** 파일이 생성됨.

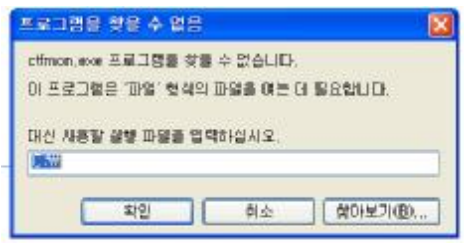
③ 하드 디스크의 **Root**폴더에 시스템 파일, 숨김 속성으로 **Autorun.inf** 을 생성.

④ **autorun.inf**의 내용.

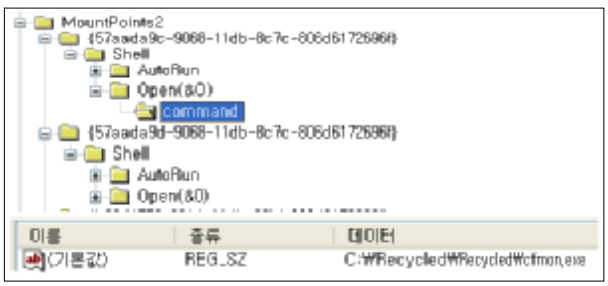
```
[autorun]
shellexecute=Recycled \ Recycled \ ctfmon.exe
shell \ Open(&O) \ command=Recycled \ Recycled \ ctfmon.exe
shell=Open(&0)
```

autorun.inf 은 자동실행을 해주는 스크립트 파일로서 보통 **CD-ROM**타이틀에서 자동으로 **CD**의 내용이 실행될 수 있도록 해주는 기능을 해주는 파일이다.
이 악성코드에서는 이 부분으로 인해 디스크 엑세스를 하거나 공유폴더를 할 경우 확산이 되는 **Trojan**류 악성코드이지만, 악성코드 자체의 위험성은 낮다.

악성코드**(ctfmon.exe)**가 프로세스에 계속 떠 있을 경우
강제적으로 악성파일을 삭제할 수 없는 상태로 되어 있으며,
또 악성코드 제거프로그램처럼 악성코드 프로세스를 죽이고 **\ Recycled**만을 제거 할 경우 디스크 드라이브를 열 때 **autorun.inf**이 자동실행되면서 다음과 같은 메세지나 엑세스 거부 현상이 일어나거나 재 감염의 원인이 된다.



이런 현상이 일어나는 경우는 아래와 같이 레지스트리
HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ MountPoints2 \ {....} \ Shell \ Open(&O) \ command
의 삭제가 제대로 되지 않았거나 각 드라이브의 **autorun.inf**를 삭제하지 않음으로 인해 문제가 된다. 이 문제는

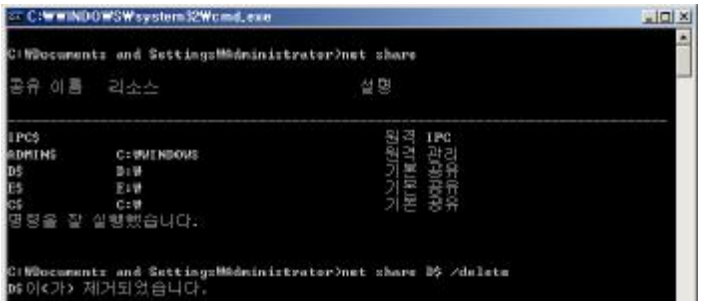


레지스트리의 **Shell**을 삭제하면 해결된다.

2. 치 료

위에서의 분석한 자료를 토대로 이 악성코드를 치료할 수 있는 방법과 이 악성코드를 제거하기 위한 백신을 만들어 보도록 하겠다.

① 모든 공유 폴더 해제

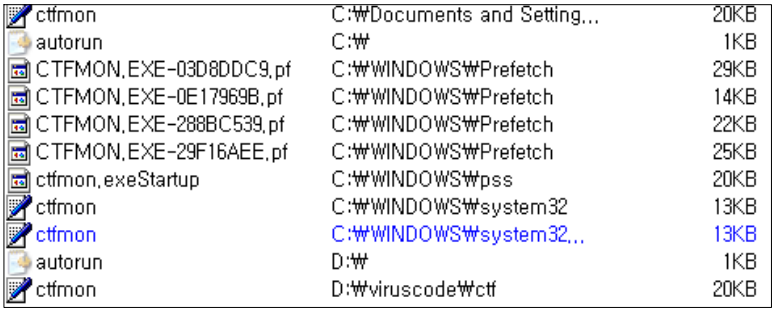


command창에서 **net share** 명령어를 실행하면 자신의 컴퓨터에 걸려있는 공유폴더 목록들이 나오게 된다.
공유 해제는 '**net share** 공유이름 **/delete**' 를 하면 해당 공유폴더가 해제된다.

② **ctfmon.exe**의 프로세스를 **Kill** 한다.

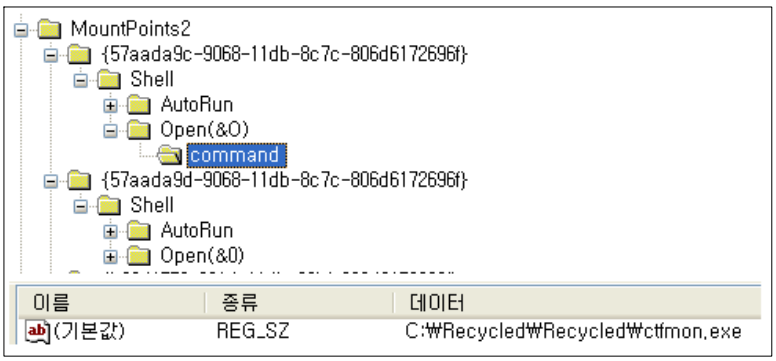
악성코드에 감염된 상태라면 **ctfmon.exe**이 **2**개 있을 것이다. **2**개의 프로세스를 **[**프로세스 끝내기**]**를 하여 프로세스를 **Kill** 한다.

③ 윈도우의 **[검색]**을 통해 **ctfmon.exe**와 **autorun.inf**을 아래와 같이 찾았다.

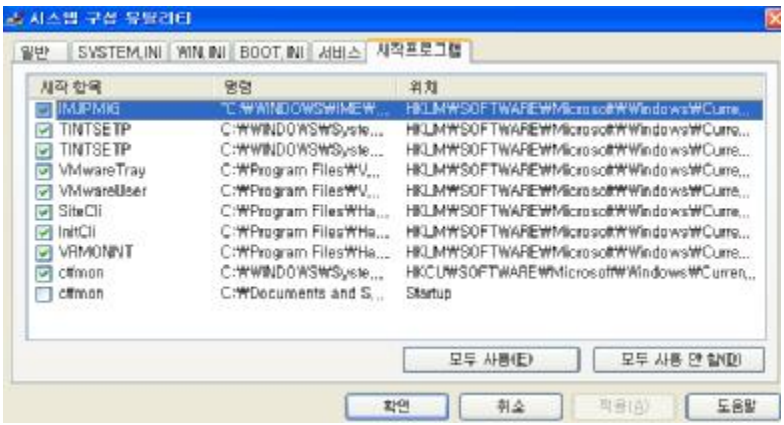


여기서 **ctfmon.exe**가 **20Kb** 인 것과 **autorun.inf**을 **Shift+Del** 을 눌러 삭제한다.

④ **regedit**를 실행시켜 **[편집]-[찾기]**에 **Open(&O)**를 찾거나 아래의 레지스트리의 위치
HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ MountPoints2 \ {....} \ Shell \ Open(&O) \ command
에서 **Shell** 자체를 삭제해 주도록 한다.

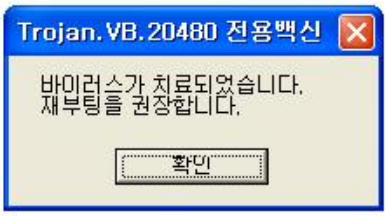


⑤ **msconfig**에서 **C: \ Documents and Settings \ ~** 에 위치가 **Startup**인 것을 해제시켜준다.

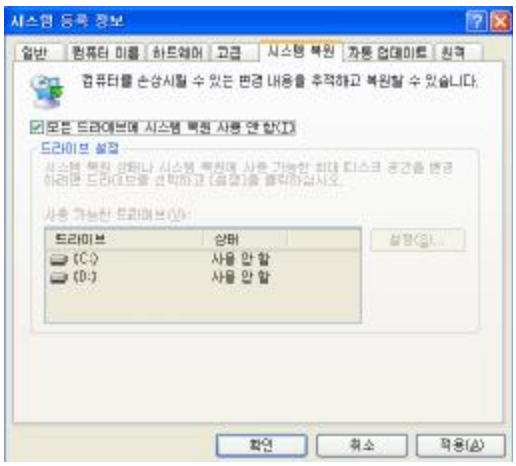


⑥ 재부팅을 하면 악성코드가 삭제되었다.

위의 방법을 모두 포함하여 아래와 같이 악성코드 제거용 백신을 만들어 보았다.
이 악성코드의 특징으로 **HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ MountPoints2** 에 존재하는 악성코드 부분을 삭제하고 악성코드 파일만 제거를 하면 되지만, 서브키를 찾아 삭제하는 방법, 시스템 숨김 파일 삭제, 연결 된 모든 디스크를 찾아내 악성코드를 제거하는 방법을 알아야 했고, 설계는 **Background**에서 사용자 몰래 치료가 되게 만들었다.
아래의 화면은 치료 후 임의로 메시지 박스를 띄어 표시한 화면이다.



⑦ 시스템 복원 기능사용 안함.



시스템 복원기능을 활성화 시켜놓을 경우 시스템 복원이 될 때 악성코드도 다시 복원되어 재감염의 원인이 되므로 꺼두는 것을 권장한다.

3. 정리 하면서...

2006년에는 제대로 치료도 못하면서 금전적 이익을 얻기 위한 거짓 안티스파이웨어로 실제 컴퓨터에는 악성코드가 없으면서도 악성코드가 있다고 잘못된 정보를 컴퓨터 사용자에에게 알려주고 치료를 하려면 '돈을 지불해야 치료가 가능하다.' 라는 등의 메시지를 자주 사용자에게 노출함으로서 사용자에게 심리적으로 불안하게 만들게 한다. 이런 피해를 막고 컴퓨터를 안전하게 사용하기 위해서는 어느 정도의 신뢰도가 있는 안티스파이웨어나 백신을 사용하길 바란다.