

오토런 바이러스 잘 잡는 방법

안녕하세요? 어베스트! 고객지원팀입니다.

본 문서는 오토런 바이러스에 대한 문의가 지속적으로 들어오는 경우가 많아 적절하게 치료하는 방법을 문서로 제공하기 위해 작성되었습니다.

자동실행(auto-run)이란?

CD/DVD, USB 메모리와 같은 이동식 매체가 삽입되면 자동으로 특정한 동작을 수행하는 기능으로 사용자의 편의를 제공하기 위해 고안되었습니다. 예를 들어, 음악 CD를 CD 롬 드라이브에 넣게 되면 자동으로 CD 재생 프로그램이 실행됩니다.

오토런 바이러스란?

오토런 바이러스는 자동 실행 기능을 이용하여 하드 디스크와 같이 다른 저장 매체를 감염시키는 악성 프로그램입니다. 최근에는 윈도우의 시작 프로그램에 등록하여 윈도우가 실행되면 자동으로 실행되어 백신이 진단하더라도 치료하거나 삭제할 수 없게 하는 경우도 많습니다.

오토런 바이러스 예방법

1. 자동 실행 기능 끄기

오토런 바이러스를 예방하는 방법은 자동 실행 기능을 꺼 주는 것입니다. 이동식 매체를 삽입하기 전에 SHIFT 키를 누른 상태에서 삽입을 하면 일시적으로 자동 실행 기능이 동작하지 않습니다. 자동 실행 기능을 사용하지 않으려면 아래의 레지스트리 키 값을 변경합니다.

HKLM / System / CurrentControlSet / Services / CDRom 에 있는 AutoRun 값을 "0"으로 변경합니다.

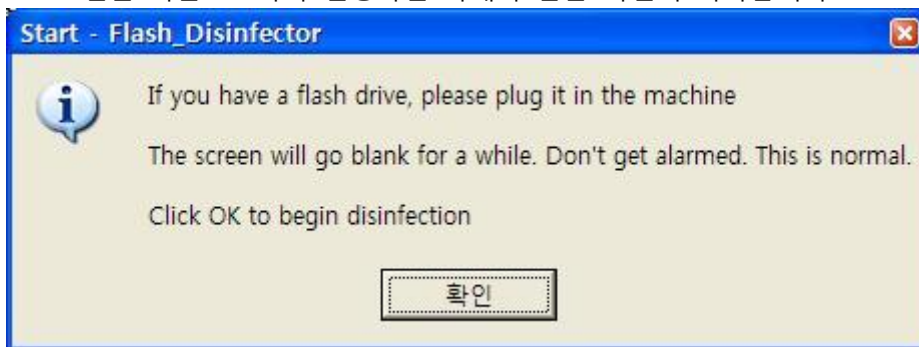
하지만, 탐색기에서 해당 드라이브를 더블클릭하거나, 엔터키를 누르거나, 또는 마우스 오른쪽 버튼을 클릭하고 자동 실행 항목을 클릭하면 자동 실행 기능이 동작하므로 주의해야 합니다.

2. 자동 실행 차단 프로그램

이동식 매체의 루트 디렉터리에는 autorun.inf 파일이 존재하며, 이 파일은 기본적으로 숨김 속성을 가지고 있어 탐색기에서 보이지 않습니다. 이 파일을 삭제하거나 동일한 파일을 두어 자동 실행을 막을 수 있습니다. 하지만 오토런 바이러스가 감염시키는 과정에서 파일을 변경할 수 있기 때문에 autorun.inf 라는 숨김 폴더를 생성하는 방식으로 자동 실행 기능을 막을 수 있습니다.

프로그램 다운로드: [Flash Drive Disinfector](#)

프로그램을 다운로드하여 실행하면 아래와 같은 화면이 나타납니다.

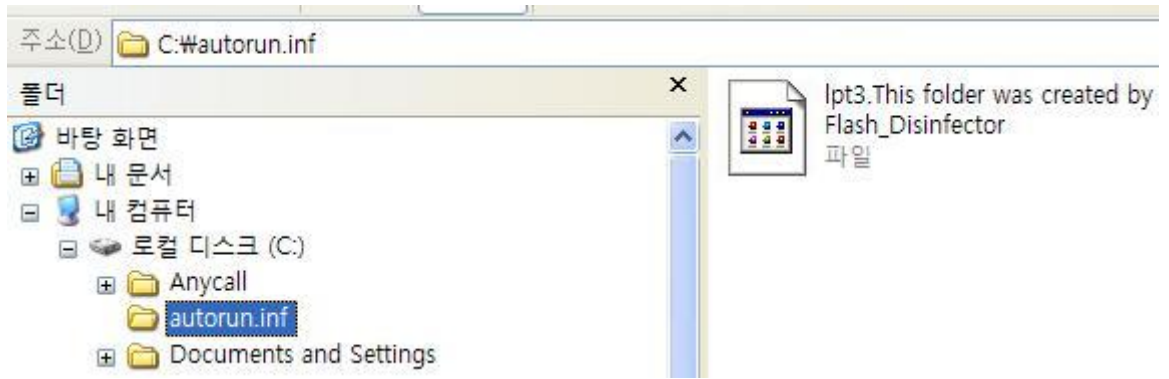


확인 버튼을 클릭하면 하드 디스크의 모드 드라이브와 모든 쓰기 가능한 이동식 드라이브(예. USB 메모리 스틱)에 autorun.inf 폴더를 생성하게 되고, 재부팅을 하게 되면 모든 작업이 완료됩니다.



주의: 각 드라이브마다 autorun.inf 폴더가 생성되어 있으므로 나중에 삭제하지 않도록 주의해야 합니다.

아래 화면은 C 드라이브에 생성된 것으로 탐색기에서 숨김 파일 보기 기능을 켜야만 볼 수 있습니다.



오토런 바이러스 감염시 증상

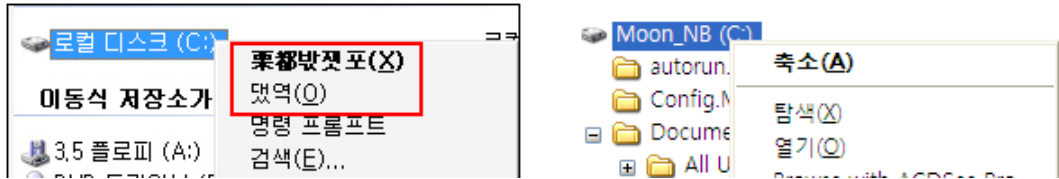
오토런 바이러스에 걸린 경우에는 보통 하드 디스크의 루트 폴더에 autorun.inf 파일이 있는지 그리고 그 파일 내에 있는 파일의 경로를 보고 확인할 수 있습니다.

만약 어베스트!에서 오토런 바이러스를 감지한 경우에는 아래와 같은 화면을 볼 수 있습니다. 진단명은 보통 Autorun, Malware-Gen 단어가 포함됩니다.



또한 탐색기에서 이동식 매체 드라이브를 마우스 오른쪽 버튼을 클릭하면 첫 번째 항목

의 메뉴가 변경된 것으로도 파악할 수 있습니다. 아래 화면에서 왼쪽에 있는 그림은 감염된 상태이고 오른쪽은 정상입니다.



알림: 팝업 메뉴의 항목이 변경되는 이유는 autorun.inf 파일 내에 포함된 특정한 속성 때문입니다. autorun.inf 파일의 형식에 대한 자세한 내용은 아래 링크를 참고하십시오.

[http://msdn.microsoft.com/en-us/library/bb776823\(VS.85\).aspx#shell](http://msdn.microsoft.com/en-us/library/bb776823(VS.85).aspx#shell)

일반적으로 어베스트!가 오토런 바이러스를 진단하여 삭제(또는 안전지대로 이동)하더라도 잠시 후에 다시 동일하게 진단하게 됩니다. 사용자 입장에서는 매우 당황할 수 밖에 없습니다.

다음에 설명하는 방법을 통해 오토런 바이러스를 완벽하게 제거할 수 있습니다.

오토런 바이러스 제거법

1. 컴퓨터에 삽입한 이동식 매체를 탈착

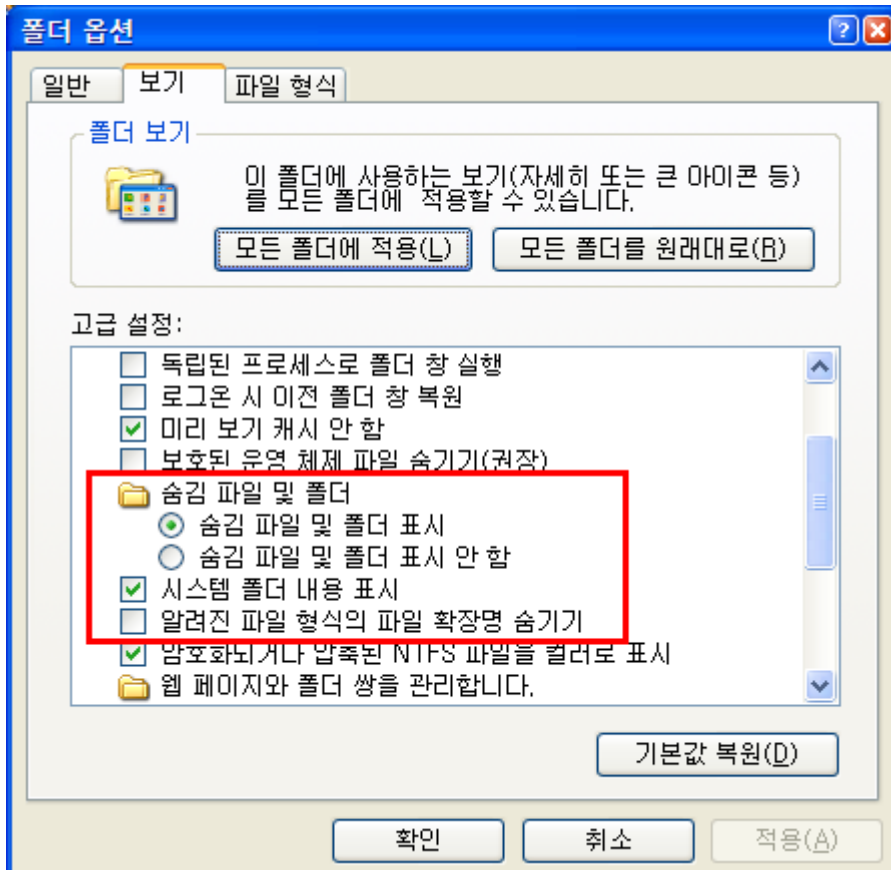
컴퓨터의 CD/DVD 롬드라이브, 플래시 드라이브, USB 메모리 스틱, 외장 하드 디스크 등등 하드 디스크 이외의 모든 드라이브를 먼저 제거합니다.

2. 안전 모드로 재부팅

컴퓨터를 재부팅합니다. 컴퓨터가 켜지기 전에 F8 키를 천천히 눌러 안전 모드를 선택하여 부팅합니다.

3. 탐색기에서 숨김 속성을 볼 수 있도록 변경

autorun.inf 파일은 기본적으로 숨김 속성을 가지고 있어 탐색기에서는 보이지 않습니다. 탐색기를 열고, 도구 -> 폴더 옵션을 클릭합니다. 그리고 보기 탭을 클릭하고 아래 화면과 같이 "숨김 파일 및 폴더 표시-선택", "시스템 폴더 내용 표시-컴", "잘 알려진 파일 형식의 확장명 숨기기-끔"을 설정합니다. 그리고 적용 -> 확인 버튼을 클릭합니다.

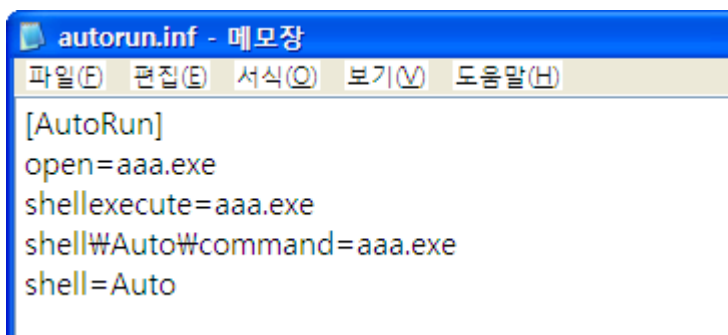


4. 탐색기에서 autorun.inf 파일 검색 및 내용 확인

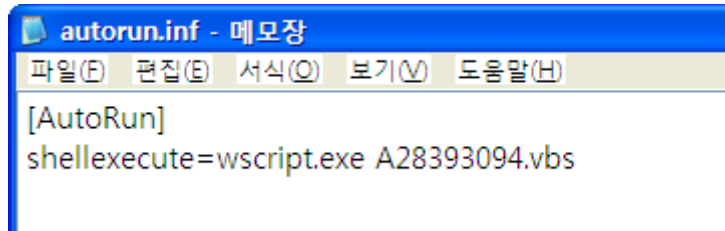
탐색기를 열고 먼저 하드 디스크 드라이브의 개수를 확인합니다. 오토런 바이러스의 특성상 모든 드라이브에 감염시키는 경우가 많기 때문에 각 드라이브마다 감염된 파일이 존재할 가능성이 높습니다.

C 드라이브의 루트 폴더로 이동하고 autorun.inf 파일을 마우스 오른쪽 버튼으로 클릭하고 **편집** 항목을 선택하여 내용을 확인합니다.

아래 그림에서와 같이 open, shellexecute, shell\Auto\command 항목에 포함되어 있는 파일 이름을 주목합니다.



만약 아래 화면과 같이 파일 확장자가 VBS와 같이 스크립트가 있는 경우에는 해당 파일의 내용 또한 확인해야 합니다.



a. 확장자가 exe인 경우

확장자가 exe, com과 같은 경우에는 해당 파일을 모두 찾아서 삭제합니다. 드라이브가 여러 개인 경우에도 모두 찾아서 삭제합니다.

b. 확장자가 vbs인 경우

작업 표시줄을 마우스 오른쪽 버튼을 클릭하여 작업 관리자 항목을 클릭합니다. 프로세스 탭을 클릭하고 wscript.exe 프로세스가 있는지 찾아 선택하고 마우스 오른쪽 버튼을 클릭하여 프로세스 끝내기를 클릭합니다.

알림: 안전모드에서는 대부분 wscript.exe 프로세스가 동작하지 않습니다.

탐색기를 열고 C:\WINDOWS\system32 폴더로 이동합니다.

wscript.exe 파일을 찾아 파일 이름을 변경하거나 확장자를 변경합니다.

주의: 변경한 파일이름은 오토런 바이러스를 모두 제거한 후에 다시 원상태로 복구해야 합니다.

이제 탐색기에서 vbs 확장자를 가진 파일을 찾습니다. vbs 파일을 마우스 오른쪽 버튼을 클릭하고 편집 버튼을 클릭합니다. vbs 파일의 내용 중에 파일 이름(경로 포함)이 있는지 자세하게 살펴 봅니다. 파일을 모두 분석한 후에는 파일 이름 목록을 따로 저장해 둡니다.

마지막으로 지금까지 알아낸 모든 파일을 탐색기에서 제거하고 컴퓨터를 다시 시작합니다. 컴퓨터는 안전 모드가 아닌 정상 모드로 부팅합니다.

어베스트!로 컴퓨터 전체를 검사합니다. 만약 아무런 악성 프로그램이 나타나지 않았다면 wscript.exe 파일의 이름을 원상태로 되돌립니다.

5. 오토런 기능 중지

앞서 설명한 3. 오토런 바이러스 예방법을 참고하십시오.

제거 이후에 다시 오토런 바이러스가 발견될 때 처리법

알림: 설명하는 내용은 컴퓨터에 대한 충분한 지식을 필요로 합니다. 잘못 설정하는 경우에는 컴퓨터에 치명적일 수도 있으므로 주의해서 사용하시기 바랍니다.

정상 모드로 부팅한 이후에 어베스트!에서 autorun에 관련된 악성 코드가 있다고 다시 진단하는 경우가 발생할 수 있습니다.

원인은 다음과 같으며 2, 3번째 원인일 경우 해결하는 방법을 소개합니다.

- 앞서 설명한 사항을 완벽하게 처리하지 못한 경우
- Userinit.exe 프로세스에 악성 프로그램에 관련된 프로세스가 등록된 경우
- 시작 프로그램 또는 특정 서비스에 악성 프로그램에 관련된 프로세스가 등록된 경우

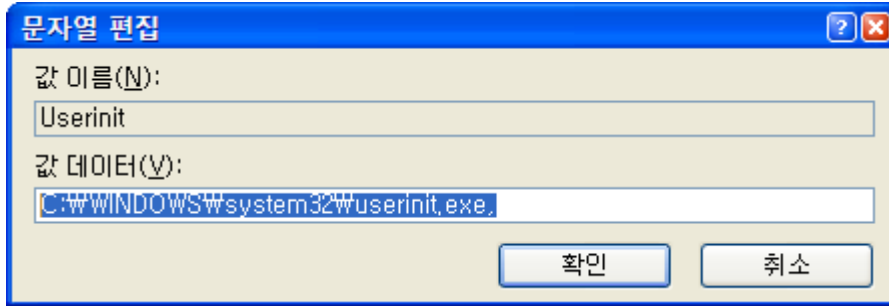
1. Userinit.exe 프로세스 확인

레지스트리 편집기(시작 -> 실행 -> *regedit* 입력 후 엔터)를 열고 아래 위치의 값을 확인합니다.

키: HKLM / SOFTWARE / Microsoft / Windows NT / CurrentVersion / Winlogon

값: Userinit

아래 화면은 정상적인 값을 나타냅니다. 마지막 부분에 쉼표(,)가 포함되어 있습니다. 또는 %System%\Userinit.exe, 값이 올 수도 있습니다.

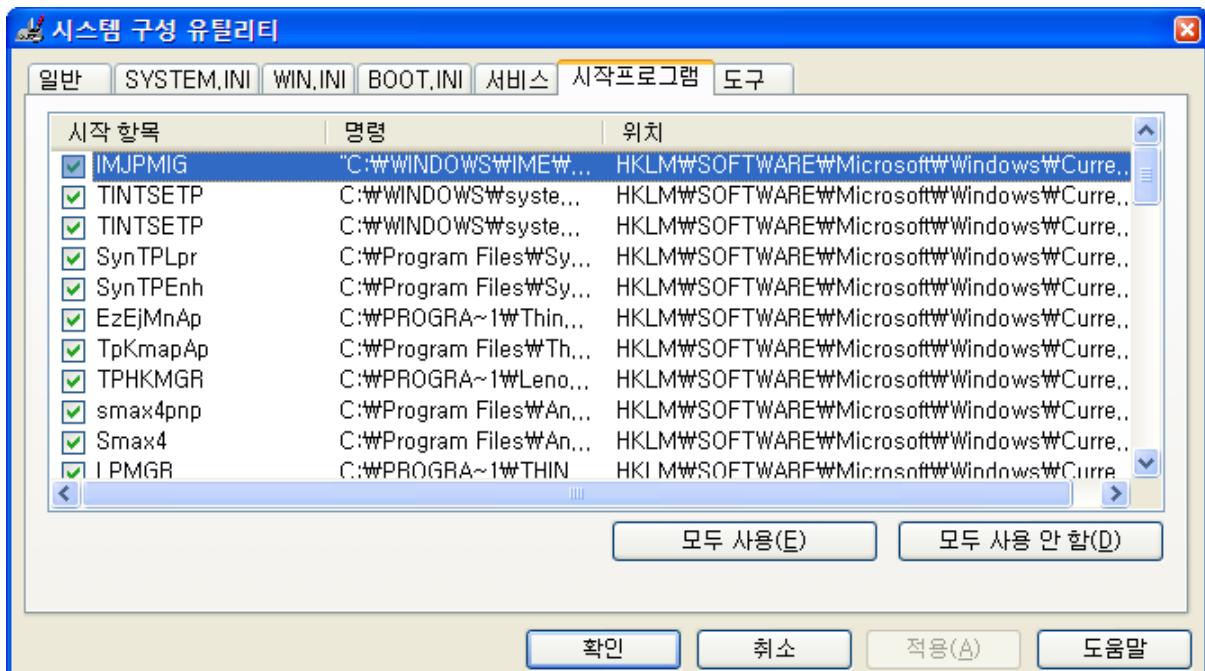


쉽표 뒤에 생소한 파일 이름이 있는 경우에는 탐색기를 열고 해당 파일을 찾아 삭제합니다. 그리고, 위 그림과 같이 쉽표까지만 놔두고 삭제하고 확인 버튼을 누릅니다.

2. 시작 프로그램 확인 - 기본

윈도우 운영체제가 부팅하는 마지막 단계에서는 사용자 또는 프로그램에 꼭 필요한 기능을 자동으로 실행할 수 있으며 보통 인터넷 연결 프로그램이나 메신저를 등록하는 경우가 많습니다.

시작 프로그램은 윈도우에서 제공하는 msconfig 명령어를 통해 쉽게 확인할 수 있습니다. msconfig 명령어를 실행하려면 **시작 -> 실행 -> msconfig** 입력 후 엔터 키를 누릅니다. 시스템 구성 유틸리티 프로그램이 실행되면 **시작 프로그램** 탭을 클릭합니다.



하지만 시작 항목을 보고 어떤 항목이 정상적인지 구별하는 것이 쉽지 않을 수도 있습니다. 시작 항목을 인터넷 검색으로 찾아 보는 것도 하나의 방법일 수도 있습니다만 가장 좋은 방법은 컴퓨터를 잘 아는 사람의 도움을 받는 것입니다.

문제가 될만한 시작 항목을 찾았다면 체크 박스를 해제하고 **적용** -> **확인** 버튼을 클릭합니다. 만약을 대비하여 별도의 장소에 변경한 사항을 적어 두는 것도 좋은 방법입니다.

3. 시작 프로그램 확인 - 고급

실제로 컴퓨터를 잘 다룰 수 있는 사용자는 앞서 설명한 msconfig 명령어보다 HijackThis 라는 프로그램을 쓰는 것이 더 효율적일 수도 있습니다. 왜냐 하면 시작 프로그램뿐만 아니라 다른 유용한 정보도 또한 볼 수 있기 때문입니다.

HijackThis 프로그램은 트렌트마이크로 社가 무료로 제공하는 프로그램으로 아래 링크에서 다운로드할 수 있습니다.

http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis

주의: HijackThis 프로그램은 Windows XP, Vista와 같은 운영체제에서 사용할 수 있으며 서버 운영체제(예. Windows 2003 Server) 등에서 대한 언급은 없습니다. 실제 사용해 본 바로는 서버 운영체제에서도 무난히 사용이 가능하지만, 문제가 생길 수 있다는 점을 명심하시기 바랍니다.

HijackThis 프로그램을 다운로드하여 실행하고 **“Do a system scan and save a logfile”** 버튼을 클릭합니다. 일련의 작업이 완료된 후에 프로그램 내에서 검사한 결과를 볼 수 있고 메모장을 통해 로그 파일로도 볼 수 있습니다. 로그 파일은 꼭 저장해야 나중에 잘못 수정한 경우에 되돌릴 수 있습니다.

로그 파일은 복잡하게 구성되어 있습니다만, 다음과 같은 항목만을 점검해도 충분합니다.

- **Running Processes** – 현재 실행 중인 프로세스 이름 및 경로를 보여 줍니다. 의심가는 프로세스가 있는 경우에는 작업 관리자에서 프로세스를 중지시킵니다. 만약 프로세스를 중지시킬 수 없는 경우에는 아래 링크에서 Process Explorer 프로그램을 다운로드하여 중지시킵니다.

<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

주의: 의심스러운 프로세스에 관련된 DLL은 검토하여 필요한 경우 파일 이름을 변경하거나 삭제합니다. DLL 파일을 잘못 변경하게 되면 시스템이 정상적으로 동작하지 않을 가능성이 있으므로 주의해야 합니다.

- **03** – 인터넷 브라우저에 등록된 툴바를 보여 줍니다.
오토런 바이러스와 관련은 거의 없습니다. 하지만, 인터넷 브라우저에 악성 코드를 삽입하거나, 쇼핑몰 적립금을 빼돌리는 악성 툴바를 찾아 낼 수 있습니다.
- **04** – 시작 프로그램에 등록된 항목을 보여 줍니다.
이 기능은 msconfig 명령어와 거의 동일합니다만 시작 프로그램에 관련된 4개의 키 값을 모두 보여주므로 더욱 효과적입니다. 시작 항목 중에 의심스러운 항목을 제거합니다.
 - ◆ HKLM\...\Run
 - ◆ HKCU\...\Run
 - ◆ HKUS\DEFAULT\...\Run
 - ◆ O4 - HKUS\DEFAULT\...\RunOnce
- **23** – 컴퓨터에 등록된 서비스의 이름 및 경로, 설명을 보여 줍니다.
사용자들이 윈도우에 등록된 서비스 이름을 모두 알 수는 없습니다. 인터넷 검색을 통해 서비스 이름과 실행 경로가 동일한지 비교해야 합니다. 참고로, 설명에 아무런 내용이 없거나 알 수 없는(깨진) 단어가 포함된 서비스를 중점적으로 살펴 보는 것도 좋은 방법입니다.

지금까지 설명한 항목을 검토하여 의심스러운 항목이라고 간주하는 경우에는 HijackThis 프로그램에서 체크하고 아래에 있는 Fix checked 버튼을 클릭합니다.

그리고 재부팅을 한 이후에 동일하게 오토런 바이러스가 진단되는지 확인합니다.

HijackThis 프로그램에 대한 자세한 사항은 아래 링크를 참고하십시오.

<http://www.bleepingcomputer.com/tutorials/tutorial42.html>

자동 실행 기능이 제대로 중지되지 않은 경우 조치 방법

3장에서 자동 실행 기능을 고도록 조치를 취한 이후에도 자동 실행 기능이 동작하는 경우에는 아래의 레지스트리 키 값을 확인하여 변경해야 합니다.

키: HKCU / Software / Microsoft / Windows / CurrentVersion / Explorer / MountPoint2

값: **!20** 으로 시작하는 클래스 ID를 클릭하고 하위 노드(shell / AutoRun / command)를 확장합니다. "a.exe"로 시작하는 문자열이 있는 경우에는 모두 삭제하고 재부팅을 합니다.

**알림: 본 문서를 사용하여 악성 프로그램을 치료하는 도중 또는 결과에 대해 보증하지 않습니다.
모든 작업을 수행하기 전에 먼저 중요한 데이터를 백업받으시기 바랍니다.**

2009년 7월 13일

어베스트! 고객지원팀 작성.