

# Antivirus Soft 치료 방법

저자: Grinler

출처: <http://www.bleepingcomputer.com/virus-removal/remove-antivirus-soft>

## 1. 소개

**Antivirus Soft**는 Antivirus Live라고 불리는 가짜 백신 중의 하나입니다. 가짜 백신은 보통 사용자의 허락없이 또는 사용자가 알지 못하는 사이에 프로그램을 설치하여 감염됩니다. Antivirus Soft는 아크로벳 리더의 예전 버전에서 발견되는 PDF 취약점을 이용하여 컴퓨터에 감염시킵니다. 설치가 완료되면, Antivirus Soft는 컴퓨터가 시작할 때마다 항상 실행되도록 '시작 프로그램' 목록에 추가합니다. 처음 실행될 때에는 컴퓨터에 악성 프로그램이 있는지 검사하고 엄청난 수의 감염된 파일을 보여줍니다. 하지만, 감염된 파일을 치료하기 위해서는 제품을 구매해야 합니다. 실제로 감염된 파일은 모두 가짜이며 컴퓨터에는 이러한 파일 자체가 없습니다.

또한, 정상적인 안티바이러스 프로그램이 Antivirus Soft를 제거할 수 없도록 자체적인 보호 수단을 가지고 있습니다. Antivirus Soft 프로세스가 실행 중일 때에는 감염되었다는 가짜 메시지를 보여주면서 다른 실행 중인 모든 프로그램을 닫게 만듭니다. 또한, Antivirus Soft는 인터넷 익스플로러의 프록시 설정을 변경합니다. 프록시 설정을 변경함으로써 Antivirus Soft 구매 사이트 이외의 다른 사이트의 접근을 방해합니다. 이런 방법으로 Antivirus Soft를 제거하는 방법이나 정상적인 안티바이러스 제품을 인터넷에서 다운로드하지 못하게 방해합니다. 이 두 가지 방법을 통해 Antivirus Soft 프로그램은 사용자가 컴퓨터를 사용할 때에 겁을 주거나 귀찮게 함으로써 구매를 유도합니다.



<그림 #1. Antivirus Soft 실행 화면.

## 2. 세부 정보

Antivirus Soft가 실행 중일 때에는 사용자의 컴퓨터에 보안 상 치명적인 문제점이 있다고 인식 하도록 다양한 보안 경고 메시지를 보여주게 됩니다. 예를 들면, 윈도우 보안 센터를 베낀 가짜 화면을 보여 주고 보안을 유지하기 위해서는 제품을 구매하게 유도합니다. 또한, 컴퓨터가 감염 되었다는 가짜 메시지를 보여 주게 되며 아래와 같이 악성 프로그램이 감염되었다고 알려주기도 합니다.

### Antivirus Software Alert

#### Infiltration Alert

Your computer is being attacked by an internet virus. It could be a password-stealing attack, a trojan-dropper or similar.

Threat: Win32/Nuqel.E

Antivirus Soft를 위협 요소에 따라 구분하면 다음에 해당합니다.

- RansomWare(사용자가 컴퓨터를 사용할 때에 팝업창을 보여 주는 것과 같이 귀찮게 하는 악성프로그램의 일종)
- Rogue(정상적인 기능을 하는 프로그램으로 보이지만 실제로는 아무런 기능을 수행하지 않는 가짜 프로그램)

Antivirus Soft의 구성요소는 다음과 같습니다.

설치되는 파일 정보	<p><b>Windows XP:</b></p> <p>%UserProfile%\Local Settings\Application Data\&lt;random&gt;\&lt;random&gt;\&lt;random&gt;\sysguard.exe          %UserProfile%\Local Settings\Application Data\&lt;random&gt;\&lt;random&gt;\sftav.exe</p> <p><b>Windows Vista and Windows 7:</b></p> <p>%UserProfile%\AppData\Local\&lt;random&gt;\&lt;random&gt;\&lt;random&gt;\sysguard.exe          %UserProfile%\AppData\Local\&lt;random&gt;\&lt;random&gt;\sftav.exe</p>
등록하는 레지스트리 정보	<p><b>Windows XP:</b></p> <p>O4 - HKLMW..WRun: [&lt;random&gt;] %UserProfile%\Local Settings\Application Data\&lt;random&gt;\&lt;random&gt;\sysguard.exe          O4 - HKLMW..WRun: [&lt;random&gt;] %UserProfile%\Local Settings\Application Data\&lt;random&gt;\&lt;random&gt;\sftav.exe</p> <p><b>Windows Vista and Windows 7:</b></p> <p>O4 - HKCUW..WRun: [ucmnrjs] %UserProfile%\AppData\Local\&lt;random&gt;\&lt;random&gt;\sysguard.exe          O4 - HKCUW..WRun:</p>

알림: 파일 및 레지스트리 정보는 HijackThis 프로그램의 로그를 이용하여 분석한 결과입니다.

### 3. 치료 방법

컴퓨터에 대한 충분한 지식이 있는 사용자는 위에서 언급한 파일 및 레지스트리 정보를 참조하여 직접 제거할 수도 있습니다만, 일반 사용자들에게는 다소 어려운 작업일 수 있습니다.

Antivirus Soft를 제거하기 위해서는 다음과 같이 3가지 사항을 반드시 명심해야 합니다.

- 치료할 때에는 안전 모드로 부팅하여 진행해야 합니다.
- 인터넷 옵션의 프록시 설정을 변경해야 합니다.
- 치료에 필요한 프로그램을 미리 준비합니다.

1) 보다 원활한 치료를 위해 본 문서를 출력하거나, 노트북과 같이 다른 수단을 준비합니다.

2) MalwareBytes' Anti-Malware(MBAM) 프로그램을 다운로드하여 바탕화면에 저장합니다. 감염된 컴퓨터에서 다운로드할 수 없는 경우에는 다른 컴퓨터에서 다운로드하여 USB 메모리 등으로 복사해 넣습니다. (프로그램은 무료 버전과 유료 버전이 있습니다. 유료 버전은 30일 평가판으로 사용할 수 있으므로 유료 버전을 다운로드합니다)

<http://www.malwarebytes.org/mbam.php>

3) 프로세스를 삭제하는 프로그램인 rkill을 다운로드하여 바탕화면에 저장합니다. 감염된 컴퓨터에서 다운로드할 수 없는 경우에는 다른 컴퓨터에서 다운로드하여 USB 메모리 등으로 복사해 넣습니다.

<http://download.bleepingcomputer.com/grinler/rkill.com>

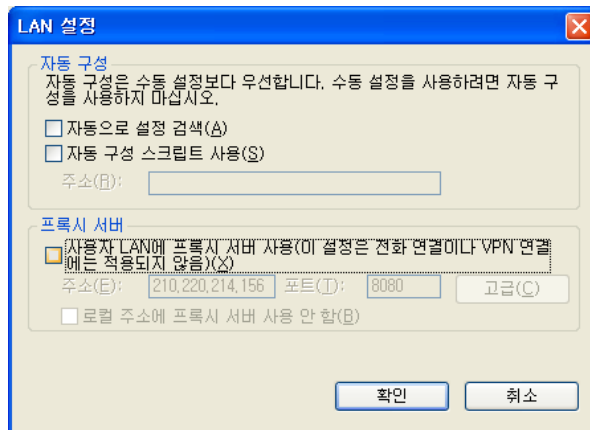
4) 이제 컴퓨터를 안전 모드로 재부팅합니다.

안전모드로 재부팅하려면 컴퓨터가 시작할 때에 F8 키를 천천히 눌러 주거나, SHIFT 키를 꾹 누릅니다.

5) 프록시 설정을 변경합니다.

시작 -> 설정 -> 제어판 -> 인터넷 옵션을 실행합니다. 연결 탭에서 LAN 설정 버튼을 클

릭합니다. 프록시 서버의 체크 버튼을 해제합니다. 그리고 확인 버튼을 눌러 창을 모두 닫습니다.



6) 실행 중인 모든 창(프로그램)을 닫습니다. 그리고, rkill 프로그램을 실행합니다. 이 프로그램은 현재 실행 중인 모든 프로그램을 닫고, 이에 대한 사항을 로그로 보여줍니다.(만약 Antivirus Soft가 감염된 프로그램이라고 경고하더라도 무시하고 실행합니다. 그런 후에 다시 한번 실행하여 완벽하게 프로그램을 닫습니다. 재부팅해서는 안됩니다.)

7) 다운로드한 MBAM(mbam-setup.exe)를 설치합니다.

설치하는 중에는 아래의 부분만 변경하고 나머지는 기본값 그대로 진행합니다.

- Update Malwarebytes' Anti-Malware 체크.
- Launch Malwarebytes' Anti-Malware 체크.

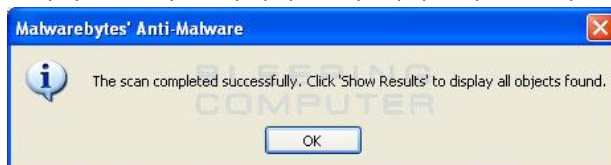
만약 설치 마지막 단계에서 재부팅이 필요하다고 대화창이 나타나더라도 재부팅해서는 안됩니다. 설치가 완료되면 MBAM이 실행되며, 자동으로 업데이트할지 묻는 대화상자가 나타는 경우에는 확인 버튼을 클릭합니다.



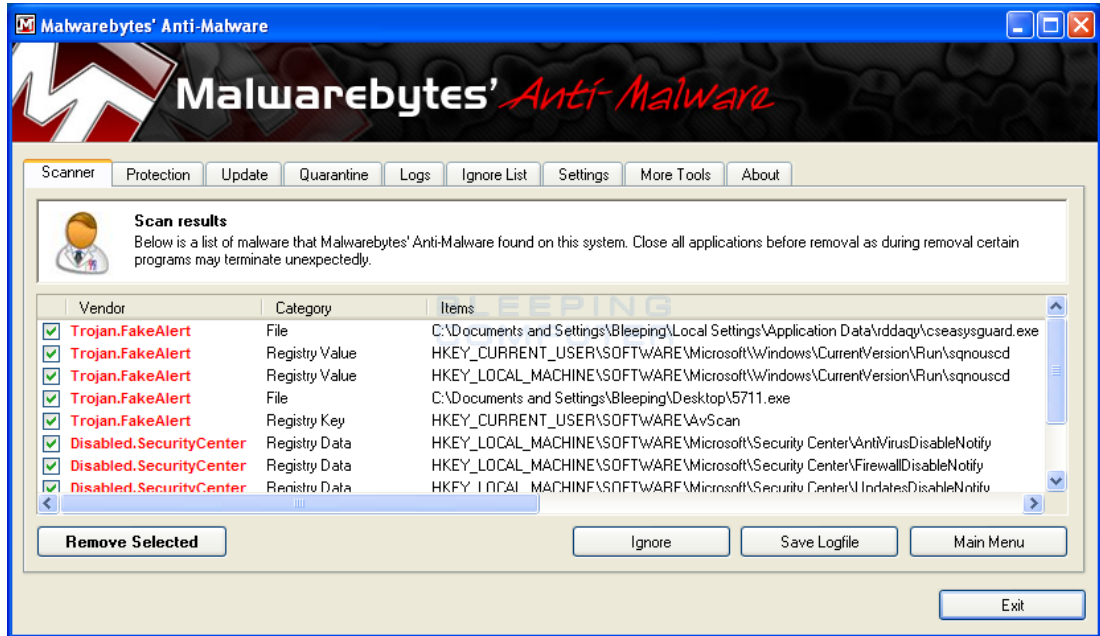
- 8) Scanner 탭에서 Perform full scan 옵션을 선택하고 Scan 버튼을 클릭합니다. 그러면, 컴퓨터에 설치되어 있는 악성 프로그램을 검사하게 됩니다. 검사하는 시간이 오래 걸릴 수도 있습니다.



- 9) 검사가 완료되면 아래와 같이 대화상자를 보여 줍니다. 확인 버튼을 클릭합니다.



- 10) Scanner 탭에서 Show Results 버튼을 클릭합니다. 그러면 아래와 같이 Antivirus Soft에 관련된 감염된 파일을 볼 수 있습니다. 아래 화면에서 일부 항목은 앞에서 언급했던 파일 이름 (경로), 레지스트리 정보와 다를 수도 있습니다.



- 11) 감염된 모든 파일을 제거하기 위해 Remove Selected 버튼을 클릭합니다. 이제 MBAM은 해당 파일과 레지스트리 정보를 모두 제거하고, 격리보관소로 옮깁니다. 만약, 제거하는 과정에서 재부팅이 필요하다고 대화창에서 표시하는 경우에는 재부팅을 하며, 이러한 경우에는 MBAM 프로그램을 실행하여 8) 단계부터 다시 진행합니다.

- 12) 모두 완료된 후에는 메모장에 로그 기록을 보여줍니다. 해당 내역을 파일로 저장하여 둡니다. MBAM 프로그램을 종료하고 재부팅합니다.

주의: 악성 프로그램은 계속 변종이 나타날 수 있으므로, 위에 언급한 사항이 100% 정확하지 않을 수 있으므로, 중요한 정보는 미리 백업하시기 바랍니다.

번역 및 정리: 문스랩닷컴(<http://moonslab.com>)