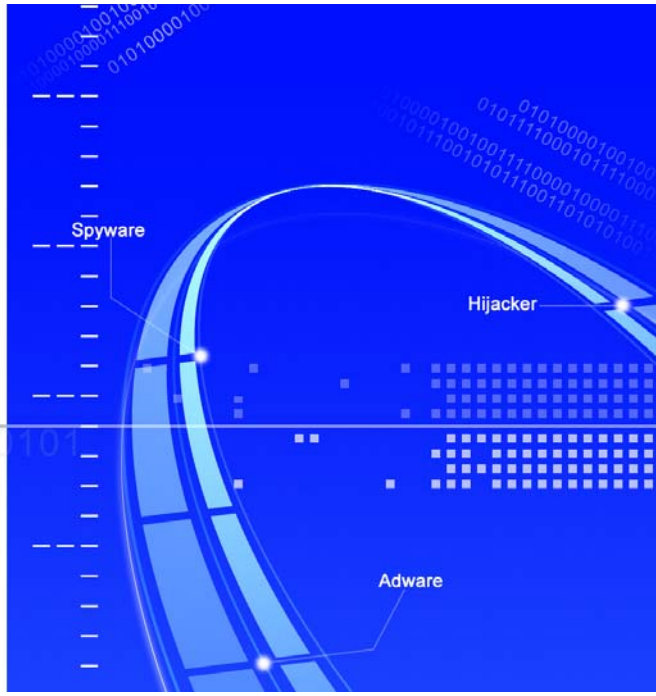
EVERYZONE

SPY VACCINE

악성코드 진단 · 치료 전문백신



사용설명서

EveryZone

시작하기 전에

고객님은 스파이백신(SpyVaccine Desktop)의 정품 사용자이십니다. 그러므로 인터넷 및 각종 환경에서 유입되는 스파이웨어 및 애드웨어와 다양한 유해 프로그램에 대응한 최선의 솔루션을 갖게 된 것입니다. 이 사용자 설명서는 스파이백신(SpyVaccine Desktop)을 사용하는데 필요한 다양한 정보를 제공해 줄 것입니다. 본 사용설명서는 1장에서는 미리 알아두기를 통하여 스파이백신을 사용하기 전 주의사항을 설명하였습니다. 2장에서 스파이백신의 간략한 소개, 특징 등을 설명하였습니다. 3장에서는 스파이백신 설치 방법이 설명되어 있으며 4장은 스파이백신의 전체적인 구성에 대해서 설명하였습니다. 5장에서는 스파이백신의 사용법을 익힐 수 있습니다. 또한 6장에서는 스파이백신 사용 시 자주 질문되는 내용을 간추려 사용자님들의 이해를 도왔습니다.

주 의

기술 및 고객지원

우편번호 : 121-719
주소 : 서울시 마포구 공덕동 253-42호 지방재정회관 17층
TEL : 02-3274-2700(대표 전화)
FAX : 02-3274-2709

목 차

1장

미리 알아두기

스파이백신 설치에 앞서 알아 두어야할
내용과 주의사항을 소개합니다.

시스템 요구사양

스파이백신(SpyVaccine) 설치에 앞서 현재 사용하는 컴퓨터 사양과 요구사양을 비교하여 프로그램 설치 및 사용에 알맞은지 반드시 확인하십시오.

CPU

인텔 펜티엄급 이상의 IBM호환 pc

RAM

128MB 이상(권장 : 256MB 이상)

HDD

15M 이상의 여유 공간

운영체제

Windows 9x/ME/2000 Professional/XP/NT WorkstationSP6 이상

정품 박스의 내용물

스파이백신(SpyVaccine) CD 1장

스파이백신(SpyVaccine) 설치 파일이 들어있는 CD

사용자 설명서

스파이백신(SpyVaccine) 설치 및 사용에 필요한 내용이 담긴 설명서

고객 등록 카드

스파이백신(SpyVaccine) 정품 등록에 필요한 카드

고객 지원 안내

에브리존은 최상의 안티 바이러스 및 안티 스파이웨어 솔루션을 제공하기 위해 최선을 다하고 있으며, 고객 상담 서비스 차원에서 전화상담 및 e-mail을 통한 친절하고 신속한 기술지원을 위해 노력하고 있습니다. 그러나 이러한 기술지원 및 고객 상담 서비스를 받기 위해서는 반드시 사용자 등록을 하셔야 합니다. 새로운 악성코드에 대한 엔진 업데이트 및 고객지원 기간은 등록 후 1년입니다. 고객지원이 만료된 후에는 1주일 간격의 정기적인 악성코드 엔진 업데이트 및 기술 지원서비스가 모두 중지 됩니다. 단, 에브리존의 백신 메일 서비스는 만료 후에도 제공됩니다.

스파이백신(SpyVaccine)은 매일 발생하는 악성코드에 대처하기 위해 매주 업데이트가 되고 있습니다. 이에 많은 인력과 개발에 비용이 투자 되고 있는 만큼 등록 유효기간이 존재 합니다. 등록기간이 만료 된 후에는 엔진 업데이트 및 각종 서비스를 받으실 수 없으므로 신종 악성코드에 대한 위험이 커집니다. 항상 최신 버전만이 새로 발견되는 신종 바이러스를 잡아 낼 수 있다는 것을 인지하시고 반드시 제품을 재 갱신하셔서 정상적인 서비스를 받으시기 바랍니다.

Tel : 02-3274-2700 (대표 전화)
FAX : 02-3274-2709

사용자 등록

고객 등록 후 지원 사항

주 1회 정기적인 악성코드 엔진 업데이트
에브리존의 백신 메일 서비스
등록 후 1년 내 제품의 업그레이드가 있을 시에 무상 제공 서비스
홈페이지 Q&A와 고객 전용 전화 / e-mail을 통한 상담 서비스
온라인 터보백신을 이용한 바이러스 무료 치료 서비스

정품 사용자 등록 방법

고객 등록 카드를 이용하는 방법

정품 패키지 내부에 포함되어 있는 고객 등록 카드를 작성하여 보냅니다.

에브리존 홈페이지를 이용하는 방법

에브리존 홈페이지(www.everyzone.com)을 이용하여 고객 전용란 메뉴를 이용하여 등록하시면 보다 신속하고 빠른 서비스를 받으실 수 있습니다.

스파이백신(SpyVaccine) 사용 시 주의사항

스파이백신(SpyVaccine)은 정품 패키지가 출시되기 전까지 알려진 스파이웨어 및 애드웨어, 각종 유해 프로그램을 진단 및 치료할 수 있습니다. 그러나 그 후에 발견된 악성코드는 진단 치료 할 수가 없습니다. 스파이백신(SpyVaccine)을 설치하고 나서 반드시 업데이트를 통해 이 문제를 해결하시기 바랍니다. 또한 스파이백신(SpyVaccine)는 신종 악성코드에 대한 정보를 추가하지 않는 이상 새로운 악성코드에 대한 대처 능력이 떨어지게 됩니다. 다른 회사의 안티 스파이웨어 제품도 이 점은 동일합니다. 스파이백신은 1주일에 한번씩 새로운 악성코드에 대한 업데이트를 제공하여 신종 악성코드에 대한 피해를 최소화하기 위해 노력하고 있습니다. 그래도 스파이백신이 진단하지 못하는 악성코드가 있다면 spy@everyzone.com에 해당 악성코드를 신고하여 주십시오. 또한 www.everyzone.com의 악성코드 신고란을 통하여 신고하여 주시면 24시간 내에 진단 치료 엔진을 제공할 것입니다. 또한 중요한 파일이나 데이터는 정기적으로 백업을 받아놓고 스파이백신을 병행하여 사용하신다면 악성코드로부터 더욱 안전한 컴퓨팅 환경을 구축할 수 있을 것입니다.


EVERYZONE

2장

스파이백신(SpyVaccine)의 소개

스파이백신(SpyVaccine)이 만들어진 배경과
주요 특징을 소개합니다.

스파이백신(SpyVaccine)에 대하여

1994년 4월에 나온 DOS용(TV.EXE) 터보백신은 1994년 10월 국내 최초의 windows용 백신으로 변모하며, 네티즌 여러분의 많은 사랑을 받아 왔습니다. 이 터보백신 엔진 기술을 스파이백신 엔진에 적용하여 예전의 이미지 그대로 강력한 기능을 보유하고 손쉬운 사용법으로 사용자 편의성을 극대화 했습니다. 스파이백신(SpyVaccine)은 인터넷 환경에 폭발적으로 증가 하는 악의적 스파이웨어와 애드웨어, 원하지 않는 팝업창과 악성 광고 싸이트로 자동 연결되는 현상을 치료 하는 전문 안티-스파이웨어 솔루션 입니다.

스파이백신(SpyVaccine)이 클라이언트 상에서 제공하는 실시간 감시기와 각종 예방 시스템은 좀 더 안전한 웹서핑을 도와드릴 것입니다.

주요 특징

스파이백신 추적 엔진(SpyVaccine Tracing Engine) 탑재

독자적으로 개발한 악성코드 검사 엔진을 이용하여 악성 코드가 이용 가능한 모든 영역을 패턴화하여 추적하는 방식으로 신뢰도 높고 정확한 진단과 치료가 가능 합니다.

운영체제 차원의 실시간 시스템 감시기능

사용자가 직접 실시간 감시수준을 3단계로 설정하여 시스템 내부 또는 외부로부터 유입되는 악성코드를 차단하며, 최적화된 설계로 다양한 시스템 성능에 부합되도록 최대한 배려하였습니다.

악성코드 예방 시스템

악의적으로 이용되었던 배포 싸이트 및 각종 데이터를 일괄 적용하여 사전 차단 및 재감염 방지가 가능하며, 또한 차단한 Active-X 컨트롤을 다시 설치할 수 있도록 복원 기능을 제공하여 사용자 편의성을 높였습니다.

시스템 정리 기능

악의적으로 이용될 수 있는 인터넷 익스플로러 정보 및 윈도우의 불필요한 파일을 제거하여 혹시라도 있을 개인정보 유출을 사전 차단하고 로컬 디스크의 공간을 확보 할 수 있습니다.

백업파일 복원 및 로그 기능

실수로 삭제한 즐겨 찾기 정보나 레지스트리 정보 및 파일을 다시 복원할 수 있으며, 로그 기능으로 자신이 주로 감염되는 악성코드 내용 및 치료 정책을 확인 할 수 있습니다.

빠르고 손쉬운 터보 업데이트(Turbo Update) 기능

최초 설치 후 자동으로 원격 터보 업데이트가 이루어지므로 사용자는 업데이트에 신경 쓸 필요가 없습니다. 또한 업데이트 주기를 설정하여 시시각각 변화하는 최신 악성코드에 대비할 수 있습니다.

직관적이고 편리한 사용자 인터페이스

사용자가 가장 많이 사용하는 기능들을 편리하게 배치하고, 단순화시키는 사용자 친화적인 GUI를 사용하여 컴퓨터 비전문가라도 쉽게 사용가능합니다.


EVERYZONE

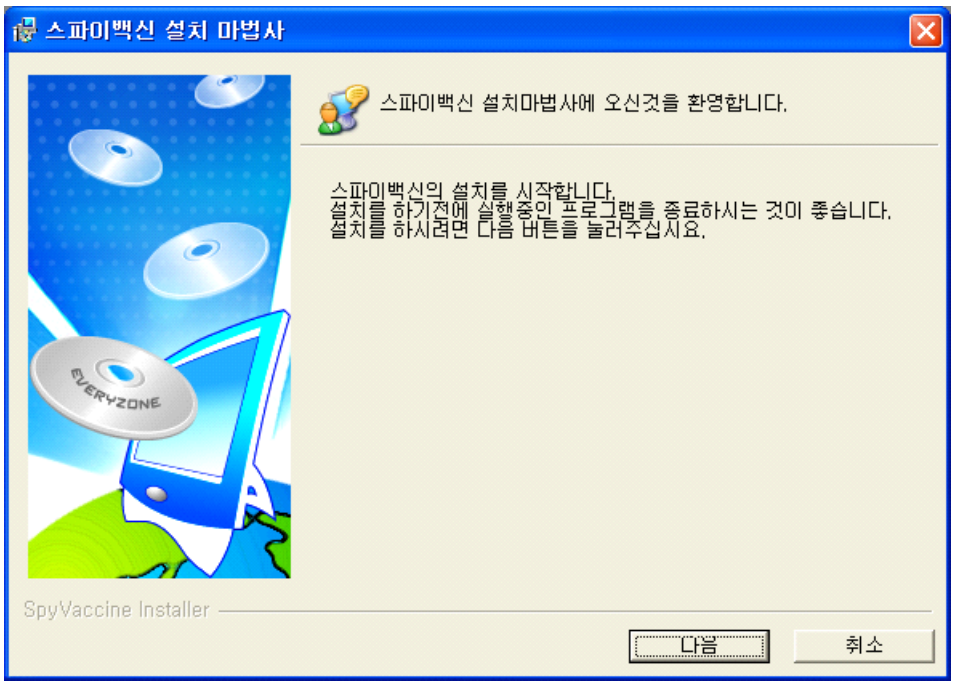
3장

스파이백신(SpyVaccine) 설치 방법

스파이백신(SpyVaccine) 설치 및
제거 방법을 소개합니다.

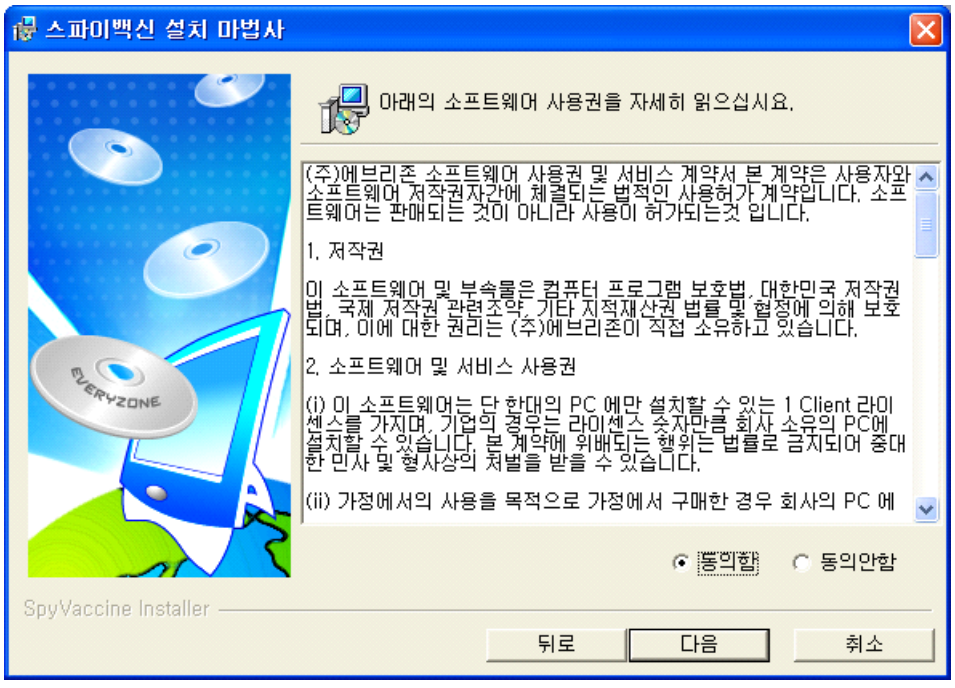
단계별 설치 절차

1. SpyVaccine.exe를 실행합니다.
2. 환영 창이 나타나면 [다음]을 누릅니다.



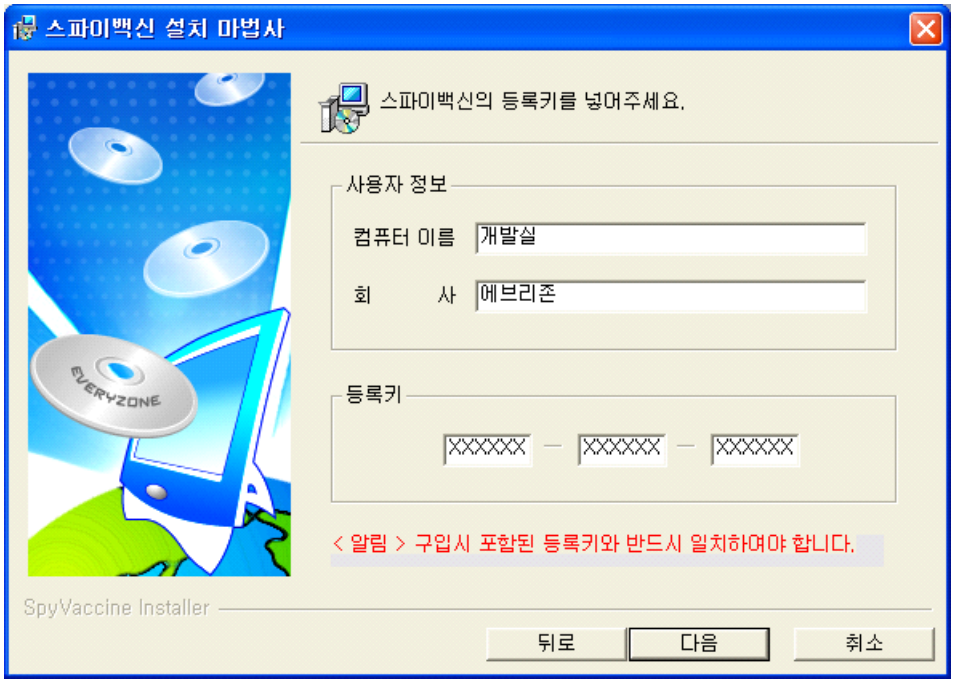
<그림1 스파이백신(SpyVaccine) 설치>

3. 소프트웨어 사용권 동의에 동의하신 후, [다음]을 누릅니다.



<그림2 소프트웨어 사용권 동의>

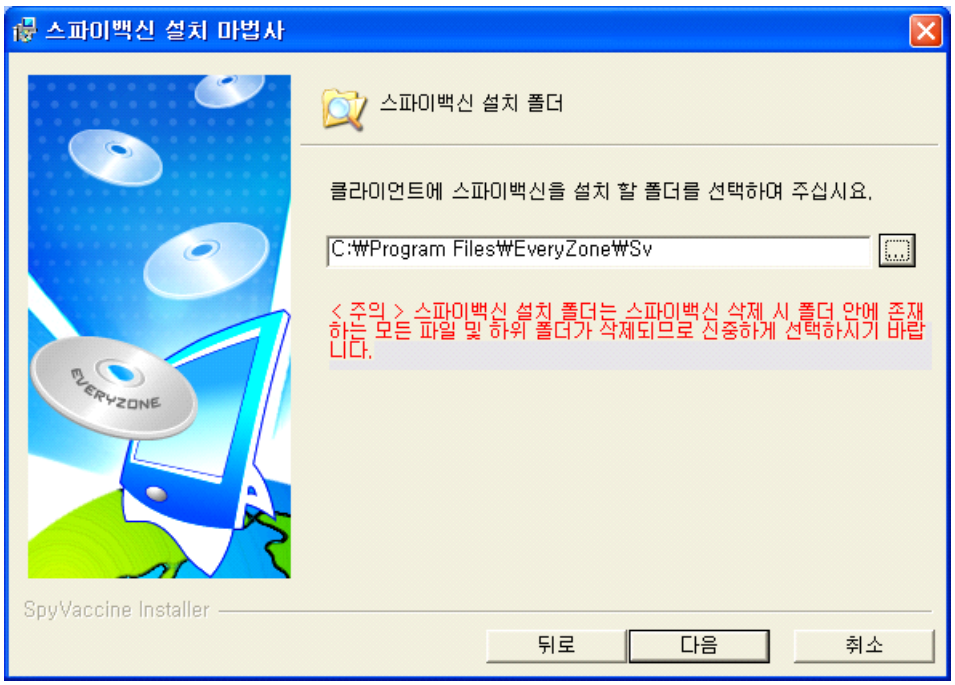
4. 등록 키 창에 CD-ROM에 동봉된 **시리얼 키를 입력**하시고 **[다음]**을 누릅니다.



<그림3 시리얼 키 입력>

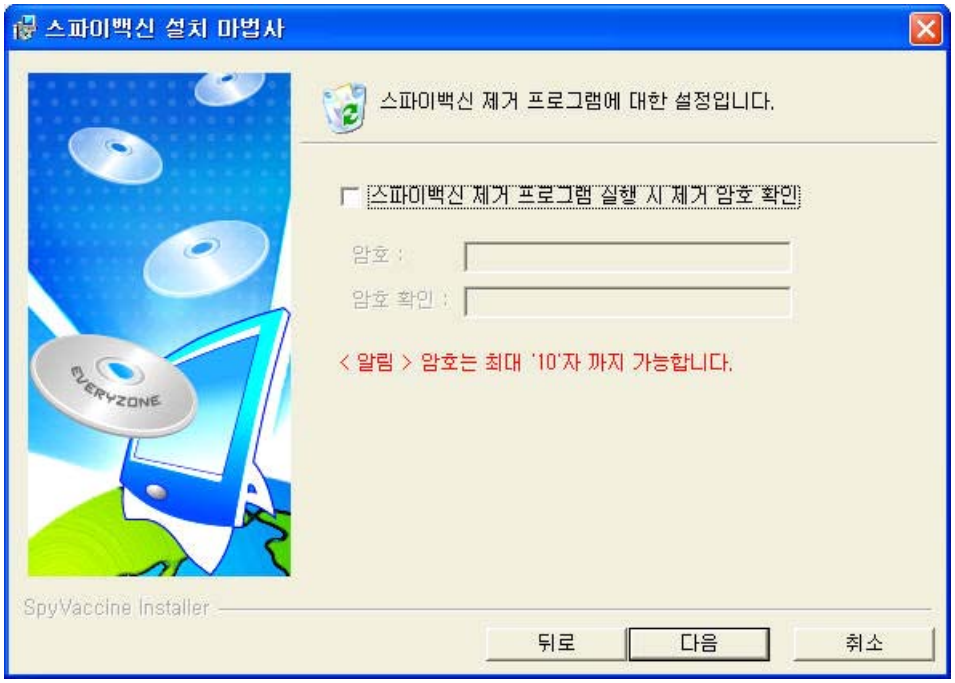
사용자 정보 중 등록 키는 꼭 넣어 주셔야 합니다. 등록 키는 동봉된 CD-ROM에 기재된 시리얼 키를 입력하시기 바랍니다.

5. SpyVaccine Desktop **설치 폴더를 선택**하시고 **[다음]**을 누릅니다.



<그림4 설치폴더 선택>

6. SpyVaccine Desktop 제거에 필요한 **패스워드를 설정**합니다.

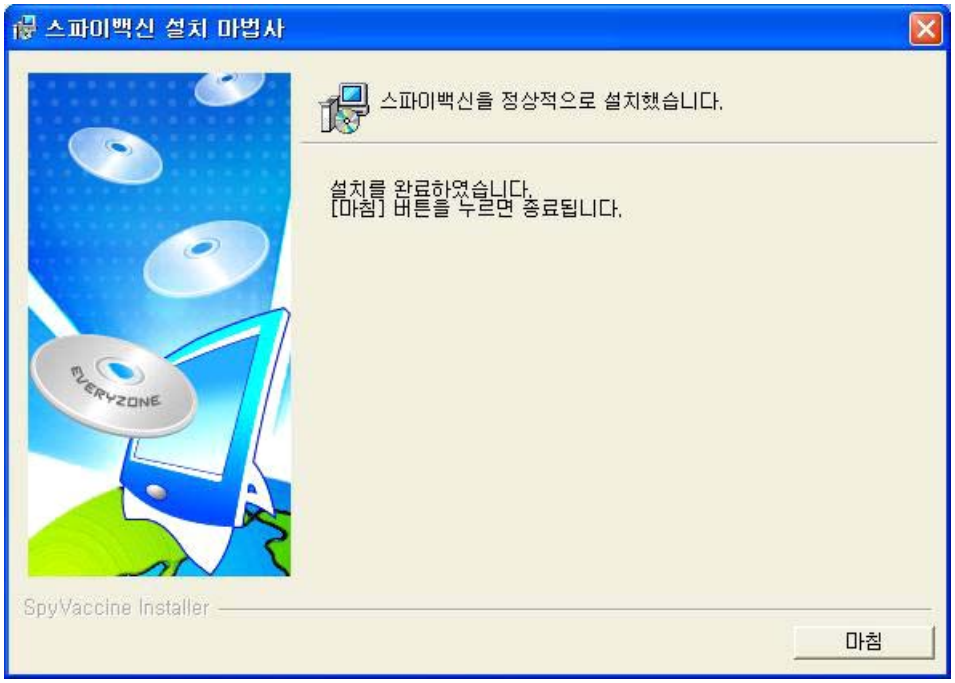


<그림5 제거 암호 설정>

7. **설치진행 화면**이 나타납니다.

<그림6 설치 진행>

8. 잠시 후 **설치 종료창**이 나타납니다.

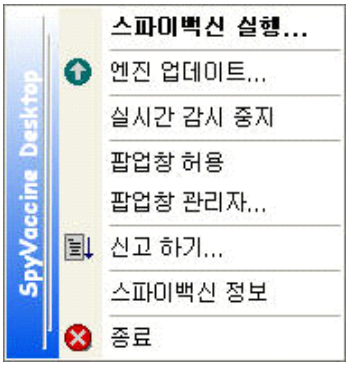


<그림7 설치 종료>

스파이백신의 설치가 끝나고 [**마침**]버튼을 클릭하면 프로그램의 설치를 완료합니다. 정상적으로 스파이백신이 설치되어 실행되었다면 **트레이에 다음과 같이 네모박스 안에 있는 아이콘이 표시**될 것입니다.

<그림8 트레이 아이콘>

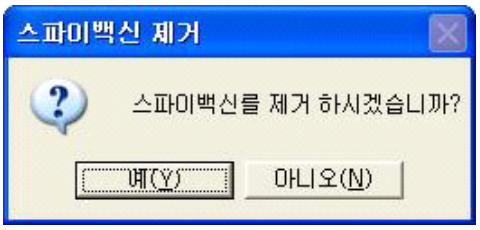
트레이 아이콘 을 오른쪽 마우스로 클릭하면 다음과 같은 메뉴가 활성화 됩니다. **스파이 백신의 주요 기능을 여기서 호출**할 수 있습니다.



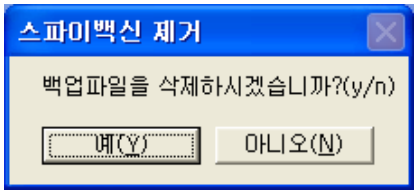
<그림9 트레이 팝업메뉴>

설치 제거하기

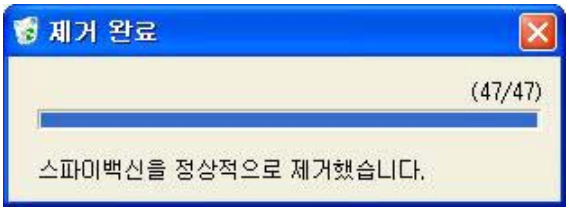
제어판의 "프로그램 추가/삭제"를 이용하시거나 [시작]->[프로그램]->[Everyzone]->[SpyVaccine]에서 "SpyVaccine 제거"를 클릭합니다.



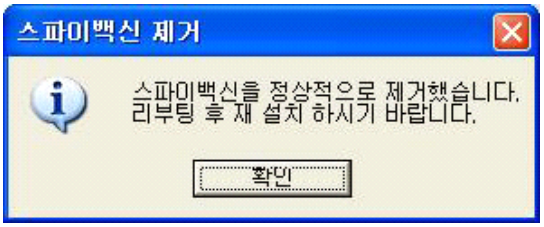
<그림10 스파이백신 제거1>



<그림10-1 스파이백신 제거2>



<그림11 스파이백신 제거3>



<그림12 스파이백신 제거4>

[확인(O)] 버튼을 클릭 하시면 스파이백신의 제거가 완료됩니다.

설치된 프로그램 폴더의 기능

스파이백신을 설치한 후 생성되는 폴더는 다음과 같습니다.

Restore

악성코드 치료 시 원래의 파일을 암호화하여 보관하는 폴더이며
[백업 휴지통]으로 해당 파일을 확인할 수 있습니다.

Log

악성코드 치료 시 해당 정보를 로그 형태로 저장합니다.
[악성코드 검사 분석기]로 확인할 수 있습니다.

Update

메일 감시기 작동 중 메일 바이러스 검사 시 메일의 원본을 임시 보관합니다.

DeActiveX

차단한 Active-X 컨트롤 모듈을 저장하는 폴더입니다.
[Active-X 차단] 메뉴에서 **[차단 목록 복원]**을 통해 확인할 수 있습니다.

Vdb

악성코드 정의가 저장됩니다.


EVERYZONE

4장

스파이백신(SpyVaccine)의 구성

스파이백신(SpyVaccine)의 화면 구성 및
툴바 기능을 소개합니다.

메인 화면

스파이백신(SpyVaccine)은 최초 **메뉴 툴바**와 **악성코드 검사 화면**으로 나누어집니다.

<그림13 메인 화면>

메뉴 툴바

스파이백신(SpyVaccine)에서 가장 사용빈도가 높은 기능을 위주로 배치하여 해당 버튼을 클릭 하는 것으로 **주요 기능을 간편하게 사용**할 수 있습니다.

<그림14 메뉴 툴바>

악성코드 검사

검사 영역을 선택할 수 있는 트리 부분, 검사 버튼과 백업 휴지통, 고급 설정 버튼, 엔진날짜, 빠른 환경설정 부분으로 구성되었으며, 엔진날짜 및 업데이트 내용을 리포트 형식으로 편리하게 확인할 수 있습니다.

Active-X 차단

인터넷 익스플로러를 통해 유입되는 유해 Active-X 컨트롤을 확인할 수 있으며, 선택 목록 차단, 차단 목록 복원, 예방 목록 설정을 이용할 수 있습니다.

시스템 정리

악의적으로 이용될 수 있는 인터넷 익스플로러 정보 및 윈도우의 불필요한 파일과 개인정보들을 제거하여 하드 디스크 공간을 확보할 수 있는 기능을 지원합니다. 또한 설치 프로그램 정리 버튼을 이용하여 현재 시스템에 설치된 프로그램을 확인할 수 있습니다.

고급 설정

엔진 업데이트 스케줄 설정 및 실시간 감시설정, 예외 설정, 로그파일 생성 옵션, 즐겨 찾기 저장 옵션 등을 제공하여 스파이 백신의 셋팅을 손쉽게 변경할 수 있습니다.

백신 업데이트

터보 업데이트(TurbuUpdate)를 호출하여 항상 최신 스파이백신으로 업데이트 할 수 있습니다.

악성코드 신고

스파이 백신에서 진단하지 못하는 내용이나 컴퓨터의 이상 증세에 대해서 질의할 수 있는 고객 지원 서비스를 별도의 메뉴를 통해 제공합니다.

악성코드 검사

<그림15 악성코드 검사>

트리영역(내 악성코드 검사, 내 컴퓨터, 내 네트워크)에서 체크를 해제하거나 추가 하는 형식으로 **검사 목록을 선택**할 수 있습니다.

악성코드 검사

레지스트리와 하드 디스크의 악성코드를 수동 검사합니다.

백업 휴지통

악성코드 검사 후 치료한 레지스트리 정보 및 파일을 다시 복원할 경우 사용할 수 있습니다.

고급 검사 옵션

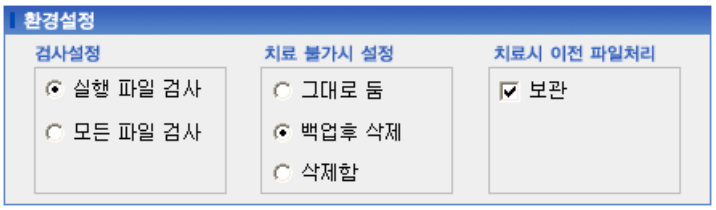
“내 컴퓨터”의 하드 디스크 전체 검사를 지원합니다. 하드디스크 파일을 검사하는 기능으로 보다 정밀한 검사가 지원됩니다.

엔진 날짜 및 내용

업데이트된 악성코드 리스트 및 날짜를 확인할 수 있습니다.

환경설정

다음처럼 악성코드 검사 시 검사 옵션을 빠르고 간편하게 설정할 수 있도록 최초 화면 전면에 배치하여 효율적인 옵션 변경이 가능합니다. 환경 설정은 [**고급 검사 옵션**]이 체크 되었을 경우 적용됩니다.



<그림16 환경설정>

실행 파일 검사

이 옵션을 선택하면 가장 빠른 악성코드검사를 수행할 수 있는 장점이 있는 반면에 실행 파일(exe, sys, dll, com, vxd)만을 검사하므로 일반적인 파일에 감염된 악성코드는 진단을 하지 못하는 단점이 있습니다.

모든 파일을 검사 합니다.

이 옵션을 선택하면 하드 디스크에 존재하는 모든 파일을 하나하나 검사하여 악성코드를 정확히 잡아내는 장점이 있는 반면에 악성코드 검사 시간이 실행 파일만 검사하는 경우에 반하여 오래 걸리는 단점이 있습니다.

그대로 둠

치료가 불가능할 경우, 감염된 파일을 삭제하지 않고 그대로 둡니다.

백업 후 삭제

치료가 불가능할 경우에는 감염된 파일을 백업 후 삭제합니다. 이 때 백업한 파일은 “백업 휴지통”을 이용하여 다시 원래의 상태로 복원할 수 있습니다.

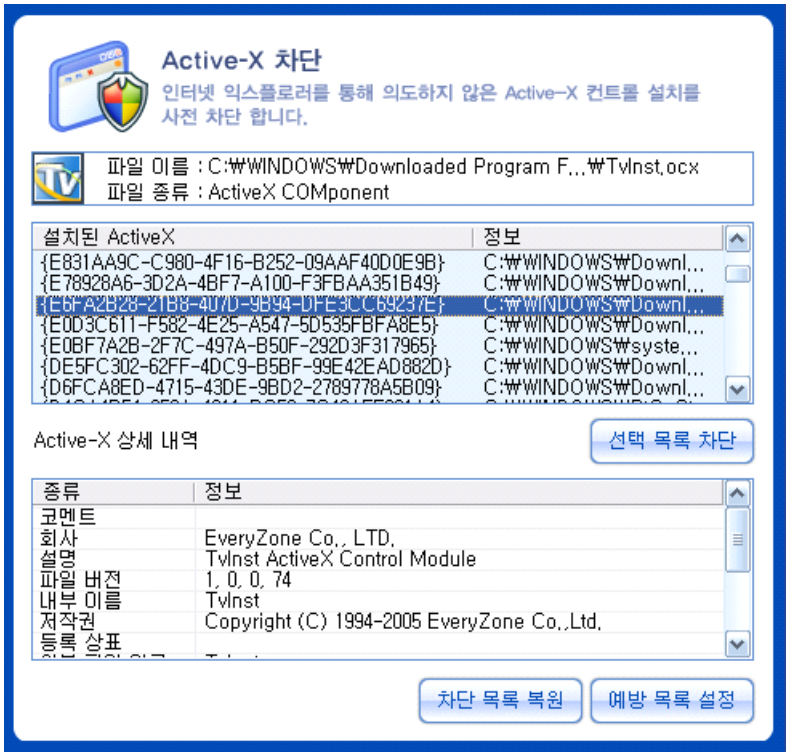
삭제함

치료가 불가능할 경우에는 감염된 파일을 영구적으로 하드디스크에서 삭제합니다. 이렇게 삭제된 파일은 다시 복구할 수 없습니다.

보관

이 옵션을 클릭 하면 발견된 악성코드를 치료할 경우에 파일이 자동적으로 보관됩니다. 보관된 파일은 [**백업 휴지통**]을 사용하여 언제든지 원래의 상태로 복원할 수 있습니다. 이 옵션은 백업 휴지통 사용방법을 참고하시기 바랍니다.

Active-X 차단



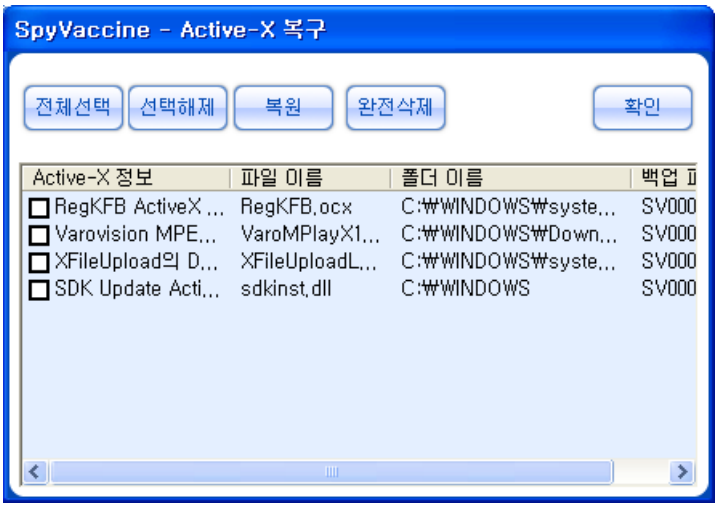
<그림17 Active-X 차단>

인터넷 익스플로러를 통해 의도하지 않은 Active-X 컨트롤 설치를 사전 차단 합니다. 기본적으로 현재 컴퓨터에 설치된 Active-X 컨트롤 목록을 보여주고 해당 목록을 선택하였을 때 상세 정보를 제공합니다.

선택 목록 차단

컴퓨터에 설치된 Active-X 컨트롤을 삭제하거나 사용 중지하고 싶을 때 이용합니다. 만약 다시 설치하거나 사용하고 싶다면 [**차단 목록 복원**] 버튼을 이용하여 컨트롤을 복원하십시오.

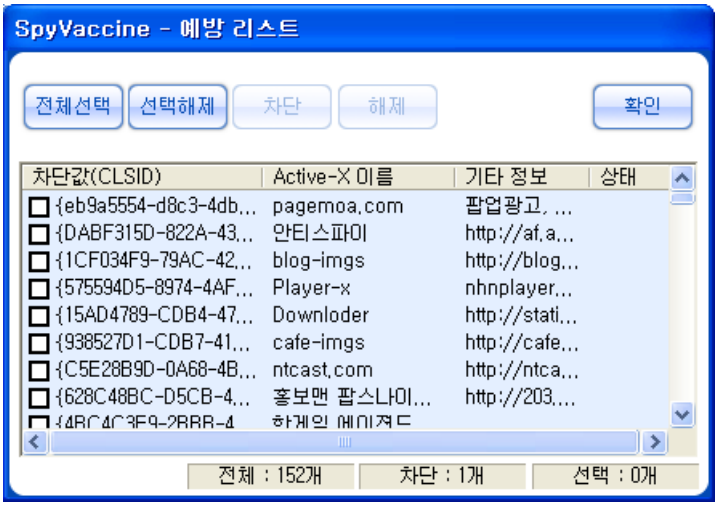
차단 목록 복원



<그림18 차단 목록 복원>

삭제한 Active-X 컨트롤을 다시 복원시킬 필요가 있을 때 사용합니다. 복원시킬 컨트롤을 [전체선택] 버튼을 이용하여 선택하거나 또는 체크박스를 직접 클릭하여 부분적인 선택하실 수 있습니다. [**완전삭제**] 버튼을 이용하면 영구적으로 컨트롤을 삭제합니다.

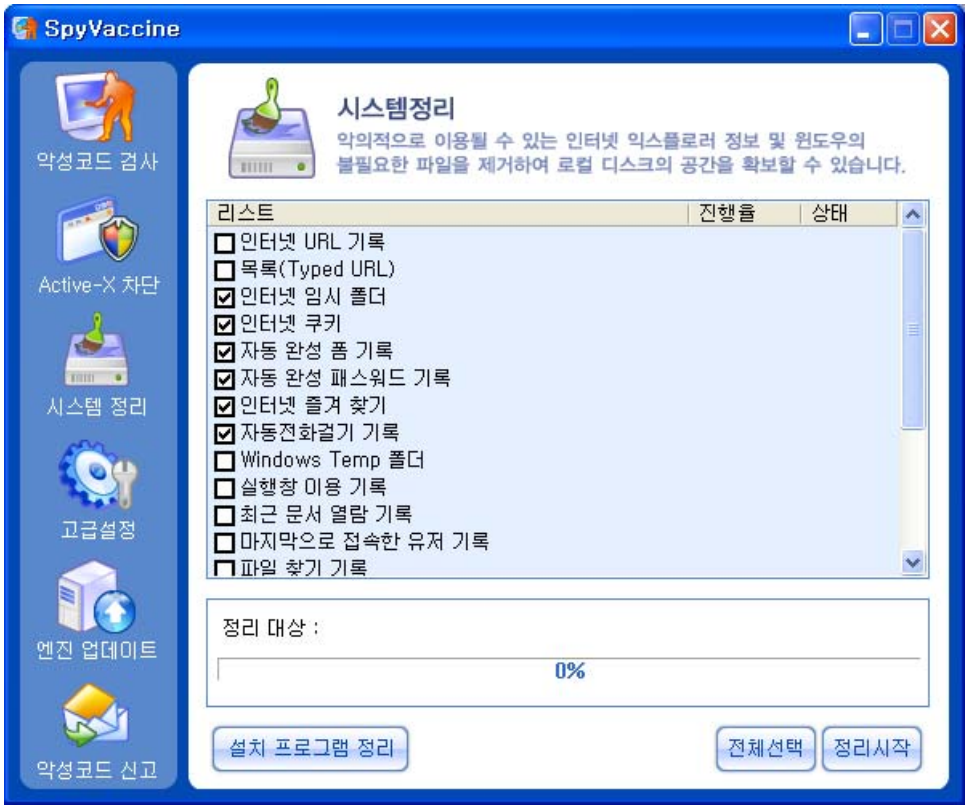
예방 목록 설정



<그림19 예방 리스트>

의도하지 않게 악의적으로 이용되었던 배포 싸이트 및 각종 컨트롤 데이터를 일괄 적용하여 사전 차단 및 재감염 방지에 주의를 기울일 수 있습니다. 해당 데이터는 고객님들의 신고 데이터 및 정보 보호 진흥원의 데이터를 참고 및 분석하여 배포되며, 최신 정보로 업데이트 시킬 수 있습니다.

시스템 정리



<그림20 시스템 정리>

악의적으로 이용될 수 있는 인터넷 익스플로러 정보 및 개인정보, 윈도우의 불필요한 파일을 제거하여 보안향상은 물론 로컬 디스크의 공간을 확보할 수 있습니다. 제거를 원하시는 목록을 체크박스를 이용해서 선택할 수 있으며, 추가적으로 로컬 디스크 공간을 확보하시려면 [**설치 프로그램 정리**] 버튼을 이용하여 시스템에 설치된 프로그램 목록을 확인후 조치를 취할 수 있습니다.

참고

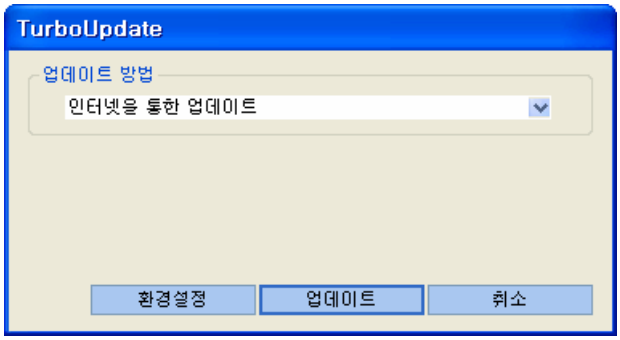
"인터넷 즐겨 찾기" 목록은 [고급설정]->[기타설정]->[즐겨 찾기 저장] 옵션에 체크되어 있으면 실수로 지운 즐겨 찾기 항목을 [**복원**] 버튼을 통해 다시 복원할 수 있습니다.

고급 설정

<그림21 고급 설정>

엔진 업데이트 스케줄 설정 및 실시간 감시설정, 예외 설정, 로그파일 생성 옵션, 즐겨 찾기 저장 옵션 등을 제공하여 스파이 백신의 셋팅을 손쉽게 변경할 수 있습니다. 설정을 변경 하신 후[**설정 적용**] 버튼을 클릭 하셔야만 변경된 옵션이 일괄 적용됩니다.

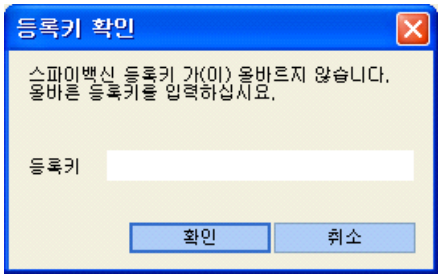
엔진 업데이트



<그림22 엔진 업데이트>

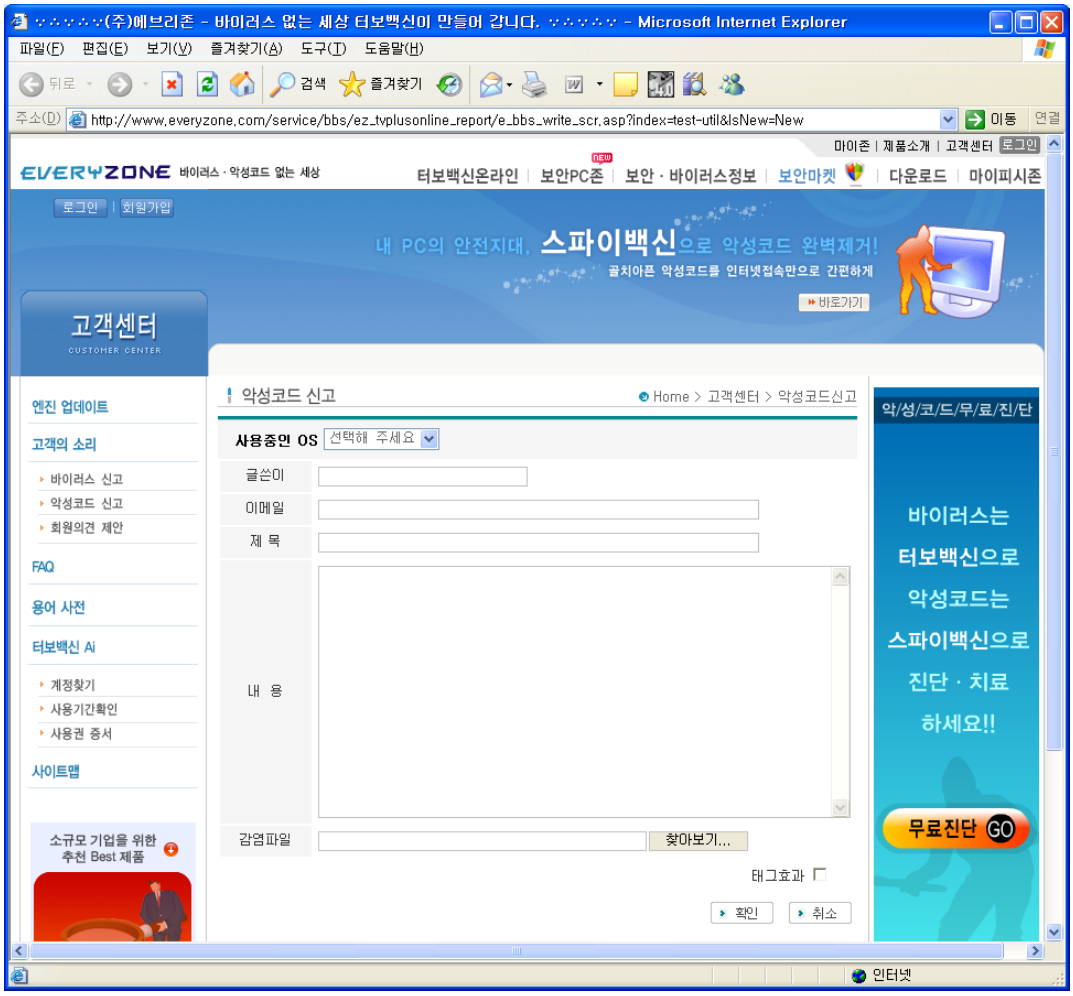
터보 업데이트(TurbuUpdate)를 호출하여 항상 최신 스파이백신으로 업데이트 합니다. 터보 업데이트(TurbuUpdate)는 에브리존 업데이트 서버 중 가장 빠른 업데이트 서버를 자동으로 찾아 신속한 업데이트를 가능하게 합니다.

인터넷 연결이 불안정하거나 혹은 업데이트 서버에 문제가 있을 경우 다음과 같은 메시지가 출력되며, 등록 키 재입력을 요구합니다.



<그림23 등록키 확인>

악성코드 신고



<그림24 악성코드 신고>

에브리존 악성코드 신고센터로 연결되어 스파이 백신에서 진단하지 못하는 내용이나 컴퓨터의 이상증세에 대해서 질의할 수 있습니다. 접수된 내용은 24시간 내에 분석되어 고객님의 이메일 주소로 답변을 보내드립니다.


EVERYZONE

5장

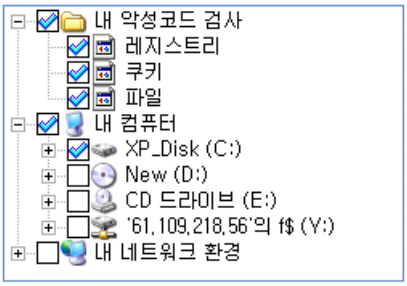
스파이백신(SpyVaccine)의 사용방법

스파이백신(SpyVaccine)의 세부적인
사용 방법을 소개합니다.

악성코드 검사 방법

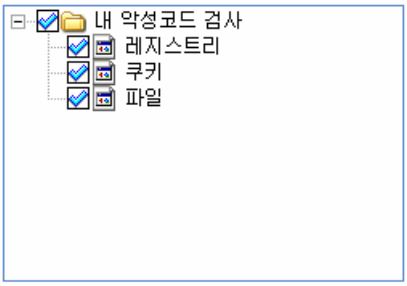
악성코드 검사는 다음처럼 두 가지 방법을 선택 할 수 있습니다.

☑ 고급검사 옵션이 체크되며 트리 영역에서 "내 악성코드 검사"와 검사하길 원하는 "내 컴퓨터"의 하드디스크나 폴더를 선택 할 수 있습니다.



<그림25 고급 검사 옵션1>

☑ 상태는 **내 악성코드 검사**와 **로컬 디스크(C:)**를 선택한 모습입니다. ⊞ 기호를 클릭하면 폴더를 선택할 수 있습니다. **고급 검사** 옵션을 선택하면 내 악성코드 검사만을 선택 한 상태보다 검사시간은 오래 걸리지만 로컬 디스크내의 모든 파일을 대상으로 악성코드를 검사하기 때문에 보다 정밀한 검사를 수행할 수 있습니다. 최초 기본 값은 고급검사 옵션이 체크됩니다. 일반 검사 시 트리 모습은 다음과 같습니다.



<그림26 고급 검사 옵션2>

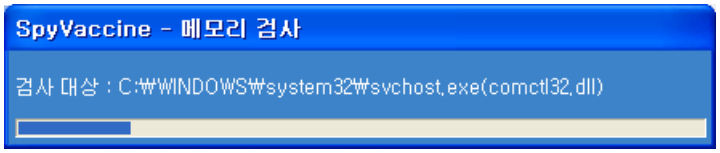
검사 시간은 가장 빠르며, 신속한 진단 치료가 필요할 때 선택합니다.

이 상태에서 

버튼을 클릭하시면 악성코드 검사를 시작합니다.
악성코드 검사 중 고급 검사 옵션이 체크된 상태라면 환경 설정 옵션의 영향을 받습니다. 현재 환경 설정 부분을 확인하신 후 옵션을 변경할 수 있습니다.

악성코드 치료 방법

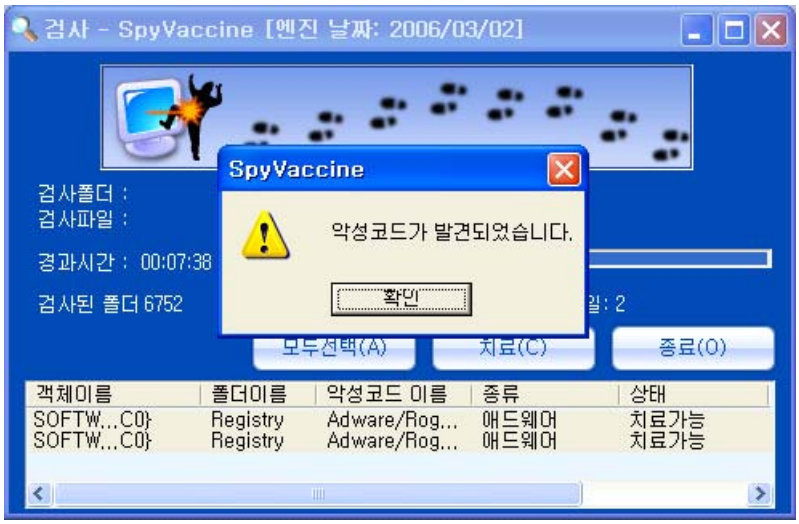
1. 검사를 시작하면 다음과 같은 창이 뜨게 됩니다.



<그림27 메모리 검사>

<그림28 악성코드 검사>

2. 이 상태에서 악성코드를 발견하면 다음과 같은 창이 뜨게 됩니다.



<그림29 악성코드 발견>

3. 악성코드를 발견하면 [**모두선택**] 버튼을 클릭합니다. 또는 CTRL키나 SHIFT키를 이용하여 치료할 파일을 개별적으로 선택할 수 있습니다.

<그림30 악성코드 검사 완료>

4. [**치료**] 버튼을 클릭하면 악성코드 치료가 완료됩니다.

<그림31 악성코드 치료 완료>

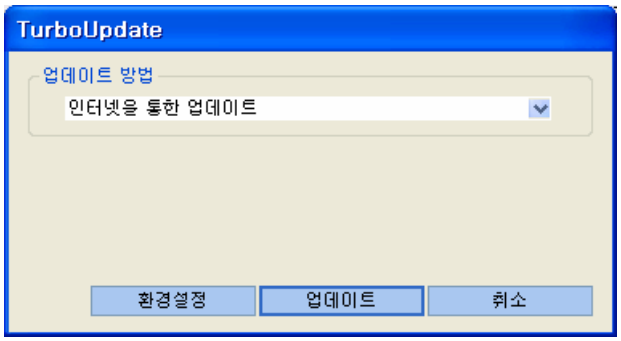
참고

악성코드 치료 후에는 치료된 파일이 환경설정 옵션에 따라 자동 저장됩니다. 이 파일은 백업 휴지통 버튼을 사용하시면 다시 복원할 수 있습니다.

스파이백신(SpyVaccine) 업데이트 방법

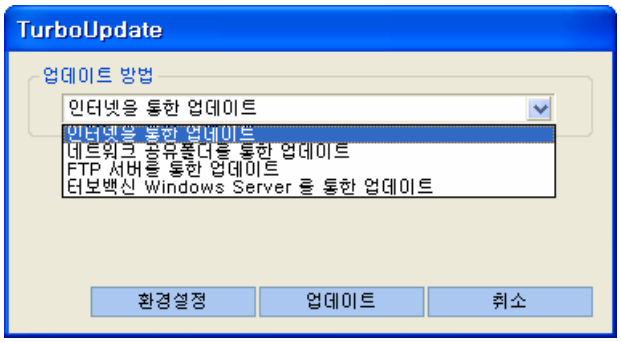
1. 

버튼을 클릭하면 다음과 같은 터보 업데이트 박스가 나옵니다.



<그림32 터보 업데이트 실행화면>

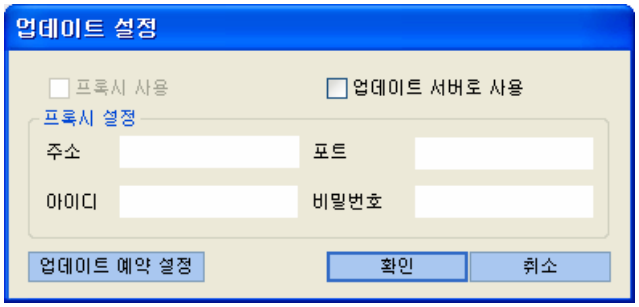
2. [**업데이트**] 버튼을 클릭하면 everyzone 업데이트 서버에서 가장 빠른 서버를 자동으로 확인하여 신속하게 최신 악성코드 엔진을 업데이트합니다.



<그림33 터보 업데이트 방법>

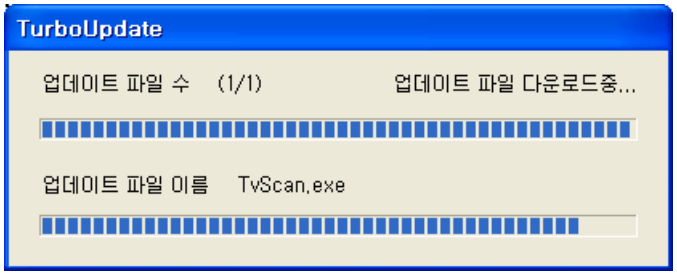
업데이트 방법에는 **[인터넷을 통한 업데이트]**와 **[네트워크 공유폴더를 통한 업데이트], [FTP 서버를 통한 업데이트], [터보백신 Windows Server를 통한 업데이트]** 방법을 지원합니다. **[인터넷을 통한 업데이트]** 방법이 기본 값이며 에브리존 업데이트 서버에 접속할 수 있는 컴퓨터 환경에 사용됩니다. **[네트워크 공유폴더를 통한 업데이트]**를 이용한 업데이트는 다른 컴퓨터의 공유 폴더에 업데이트 파일이 있는 경우 별도로 에브리존 업데이트 서버에 접속하지 않고도 최신 악성코드 정의를 업데이트 받을 수 있습니다. **[FTP 서버를 통한 업데이트], [터보백신 Windows Server를 통한 업데이트]**는 "터보백신 매니저 3.0" 이상의 관리 프로그램을 함께 사용할 때 적용할 수 있으며, 일반적인 환경에서는 사용할 수 없습니다.

3. 터보업데이트 창에서 [**환경설정**] 버튼을 클릭하면 업데이트 환경을 별도로 셋팅하실 수 있습니다.



<그림34 터보 업데이트 환경설정>

[업데이트 서버로 사용] 항목을 설정 하면 해당 터보백신이 업데이트 서버로 동작하여 접속된 다른 컴퓨터의 스파이백신을 자동으로 업데이트 해줍니다. 스파이백신이 설치된 컴퓨터가 서버 컴퓨터이고 여러 대의 내부 컴퓨터가 이 서버에 연결되어 있다면 별도의 스파이백신 업데이트 서버로 사용할 수 있습니다. **[프록시 사용]** 항목은 인터넷 연결이 프록시 서버를 통할 경우에 사용되며 일반적으로는 별도의 설정을 하지 않습니다.



<그림35 터보 업데이트 진행 창>

주의사항

프록시 서버를 사용하실 때는 반드시 주소와 포트를 정확히 기입하셔야하며 가급적이면 처음 설치될 때의 디폴트 설정을 사용하시기 바랍니다. 그렇지 않을 경우에는 업데이트가 정상적으로 이루어지지 않을 수 있습니다.

백업 휴지통 사용방법

버튼을 클릭하면 백업 휴지통 창이 실행됩니다. 한번이라도 스파이백신으로 악성코드를 치료한 상태라면 백업 휴지통은 다음과 같이 실행될 것입니다.

<그림36 백업 휴지통1>

위 그림에서 Tv000001.TBF는 감염된 파일을 스파이백신 고유파일 포맷으로 만들어서 저장한 형태로 악성코드로써 동작을 하지 못합니다. 이 파일들은 스파이백신이 설치된 폴더의 _Restore폴더에 존재하게 됩니다. 만일 중요한 문서나 파일을 복구할 필요성이 있을 때는 다음과 같은 절차에 따라 진행하시면 파일을 복원할 수 있습니다. 먼저 복구하기를 원하는 파일을 개별적으로 선택(CTRL키나 SHIFT키 이용) 하거나 또는 

버튼을 이용합니다.

전체선택(A) 버튼을 사용한 경우

<그림37 백업 휴지통2>

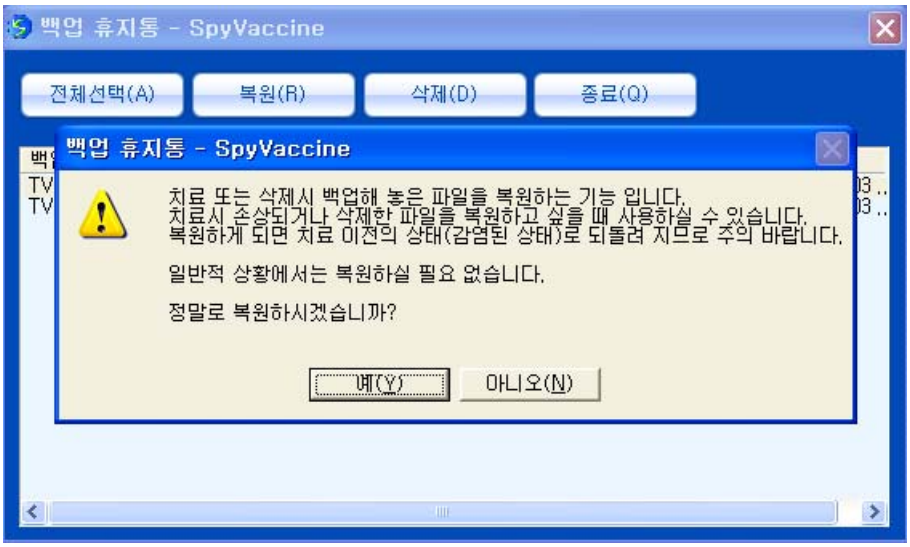
개별 선택을 사용한 경우

<그림38 백업 휴지통3>

복원

이러한 상태에서 

버튼을 클릭하면 선택한 파일을 원래의 상태로 복원하게 됩니다.



<그림39 백업 휴지통4>

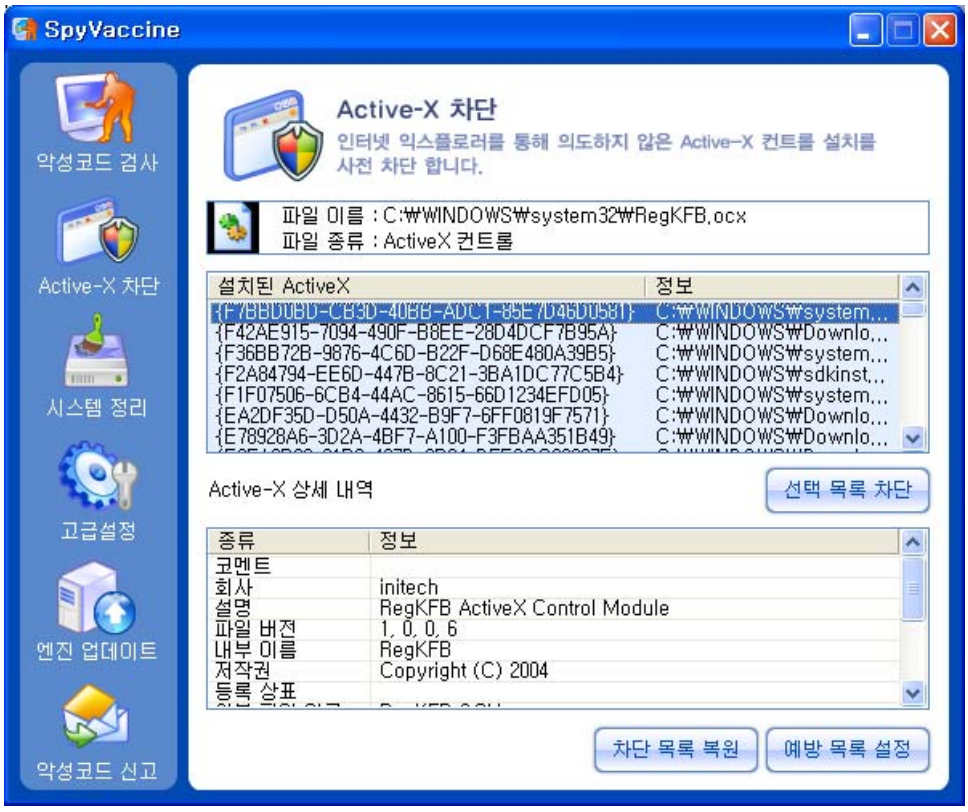
주의사항

백업휴지통으로 파일 및 레지스트리를 복원하더라도 치료 이전의 상태로 복원되므로 악성코드에 감염되어 있는 상태입니다. 그러므로 파일 및 레지스트리 정보를 복원할 경우에는 신중을 기하셔야 합니다.

Active-X 차단 방법

1. 

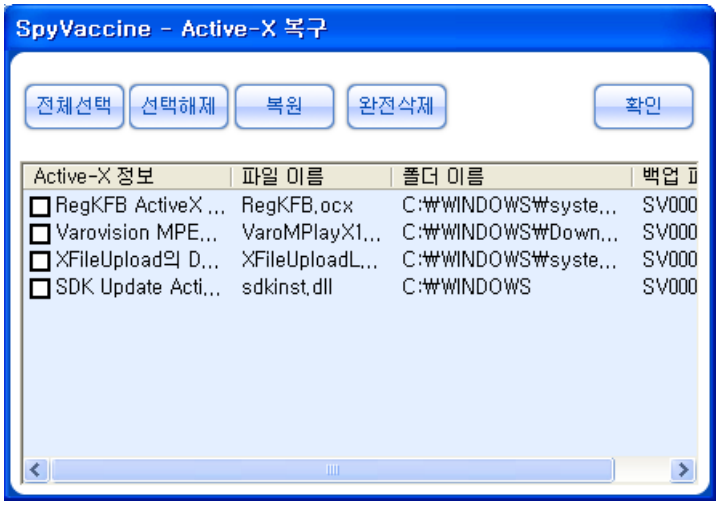
버튼을 클릭하면 다음과 같이 현재 컴퓨터에 설치되어 있는 Active-X 모듈이 표시됩니다.



<그림40 Active-X 차단>

2. 차단하기 원하는 모듈을 마우스로 선택한 후 선택 목록 차단 버튼을 클릭합니다.

3. 삭제된 Active-X 모듈은 [차단 목록 복원] 버튼을 통해 다음과 같이 확인할 수 있으며, 복원도 가능합니다.



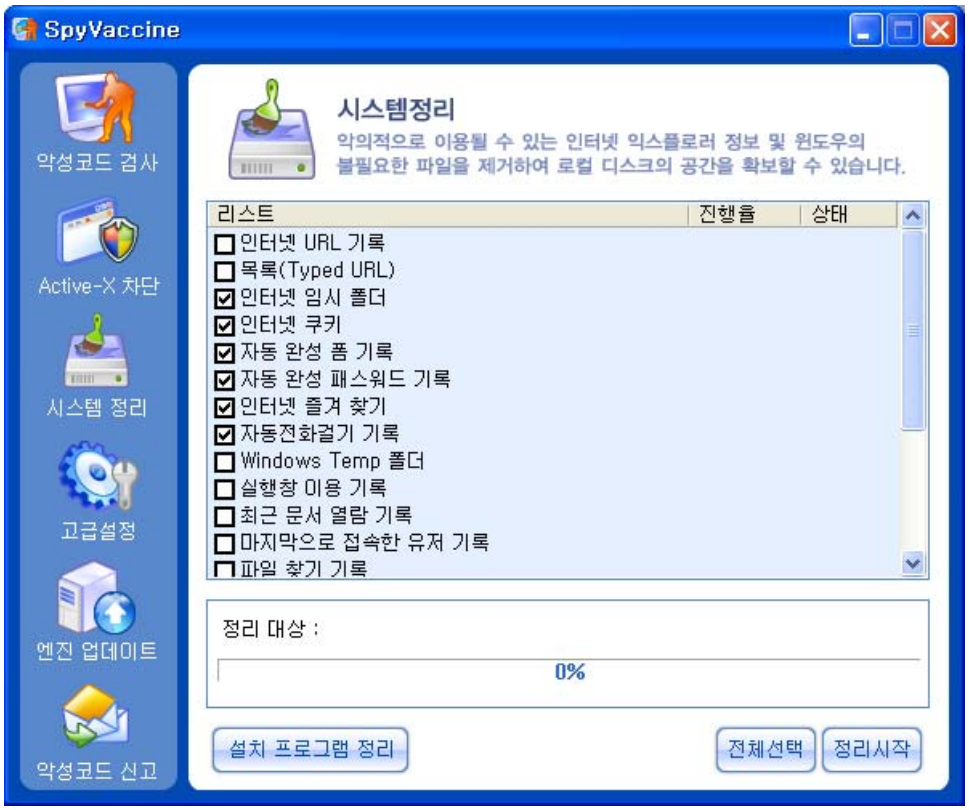
<그림41 Active-X 복구>

삭제 및 차단된 목록은 SV000000.SAB 고유파일 포맷으로 DeActiveX 폴더에 암호화되어 저장됩니다.

시스템 정리 방법

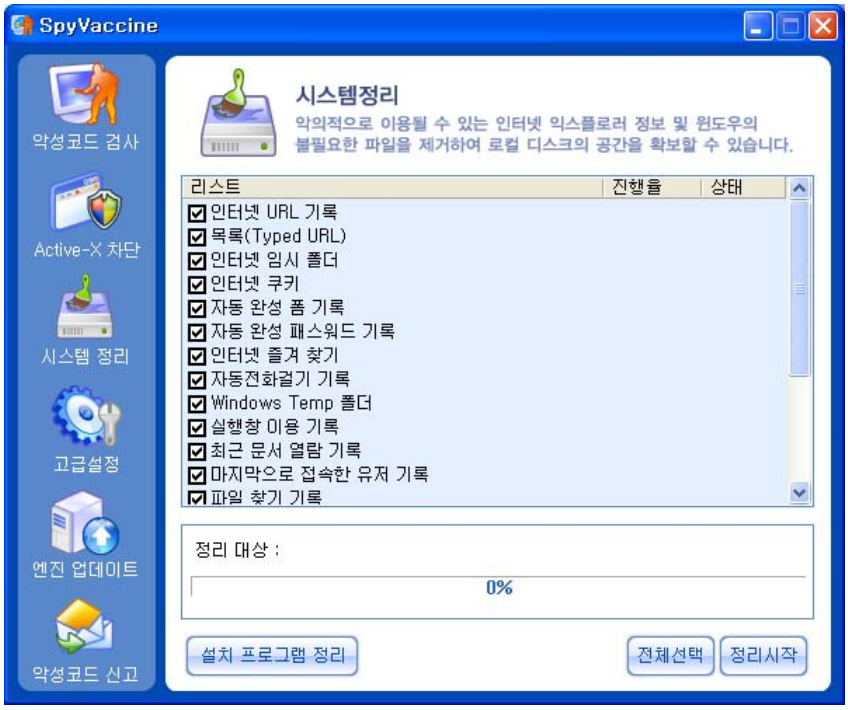
1. 

버튼을 클릭하면 다음과 같이 정리할 목록을 보여줍니다.



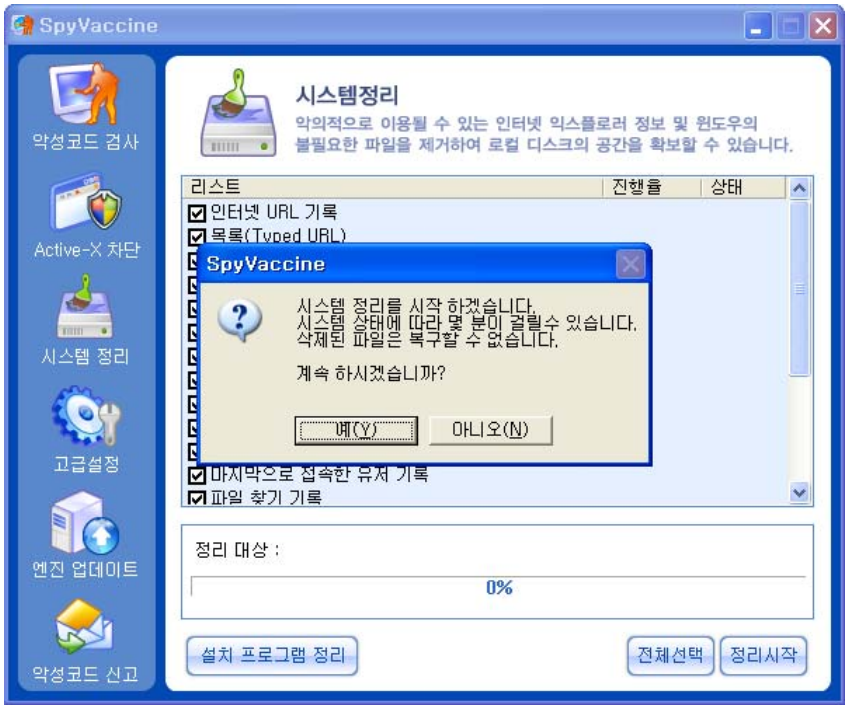
<그림42 시스템 정리>

2. [**전체선택**] 버튼을 클릭하면 다음처럼 모든 항목에 체크표시가 됩니다.



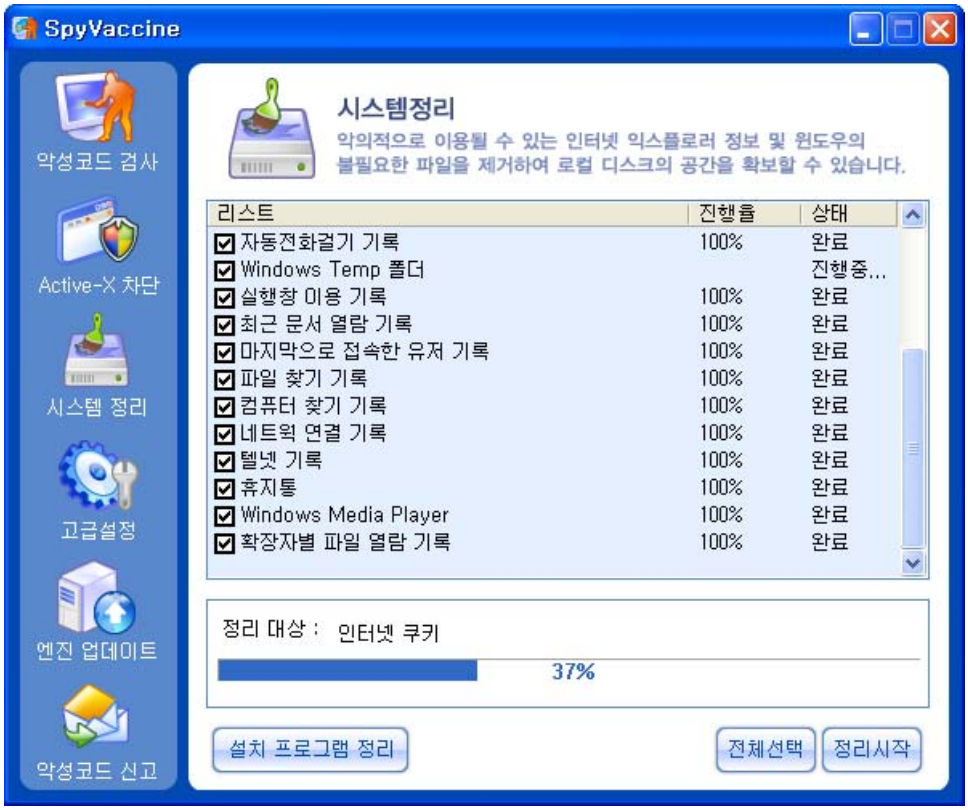
<그림43 시스템 정리1>

3. 정리를 원하지 않는 항목은 체크 표시를 선택하여 체크를 해제하십시오.



<그림44 시스템 정리2>

4. [**정리시작**] 버튼을 클릭 하면 다음처럼 시스템 정리가 시작됩니다. 정리가 끝난 항목은 "진행률" 란에 "100%", "상태" 란에 "완료" 표시가 됩니다.



<그림45 시스템 정리3>

[설치 프로그램 정리]는 현재 윈도우에 설치된 프로그램 목록을 보여줍니다. [제어판]->[프로그램 추가/삭제]와 동일합니다.

고급 설정 사용 방법

버튼은 스파이백신(SpyVaccine)의 주요 기능을 시스템 성능에 따라 변경이 가능하도록 옵션 변경 기능을 제공합니다.

<그림46 고급 설정>

업데이트 설정

터보 업데이트(TurboUpdate) 프로그램 실행 상태 옵션을 변경합니다.

새 업데이트 내역 표시

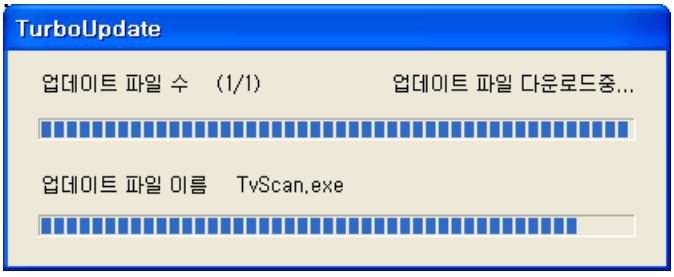
터보 업데이트가 악성코드 정보 업데이트를 완료하면, 업데이트된 내용을 TXT 파일 형식으로 노트 패드를 이용해 보고합니다. 체크를 해제하면 업데이트 후 새로운 업데이트 정보를 보고하지 않습니다. 업데이트 내역을 볼 필요가 없을 때, 이 옵션을 적용합니다.

부팅 시 자동 업데이트

컴퓨터를 재부팅 할 때마다 터보 업데이트 작동 유무를 결정합니다. 기본 값은 체크된 상태이며, 부팅 시 스파이백신의 업데이트에 신경 쓰고 싶지 않을 때 사용합니다. 수동으로 업데이트 하는 방법은 [스파이백신 업데이트 방법]을 참고하시기 바랍니다.

업데이트 창 보이기

터보 업데이트가 실행될 때 새로운 업데이트 내용을 서버에서 내려받을 경우 다음과 같은 업데이트 창을 보여줍니다.

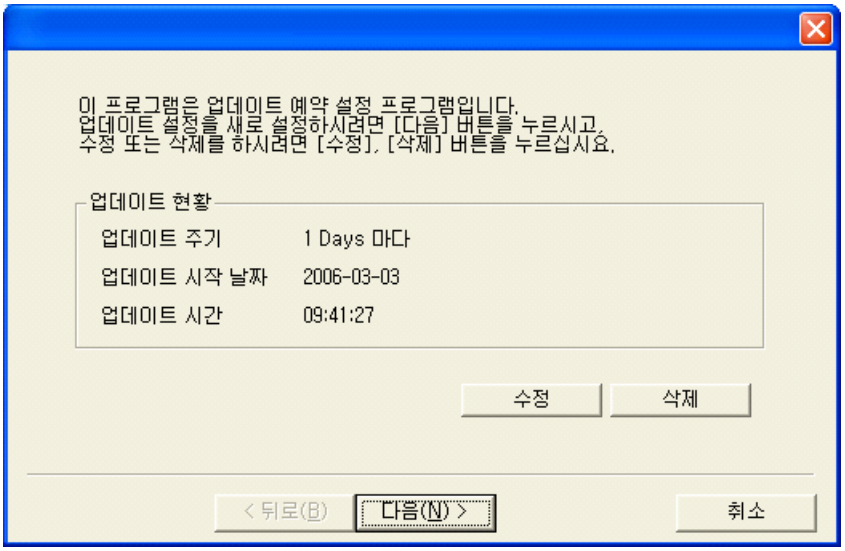


<그림47 업데이트 진행창>

체크를 해제할 경우 백그라운드로 업데이트가 이루어지므로 별도의 창이 뜨지 않습니다.

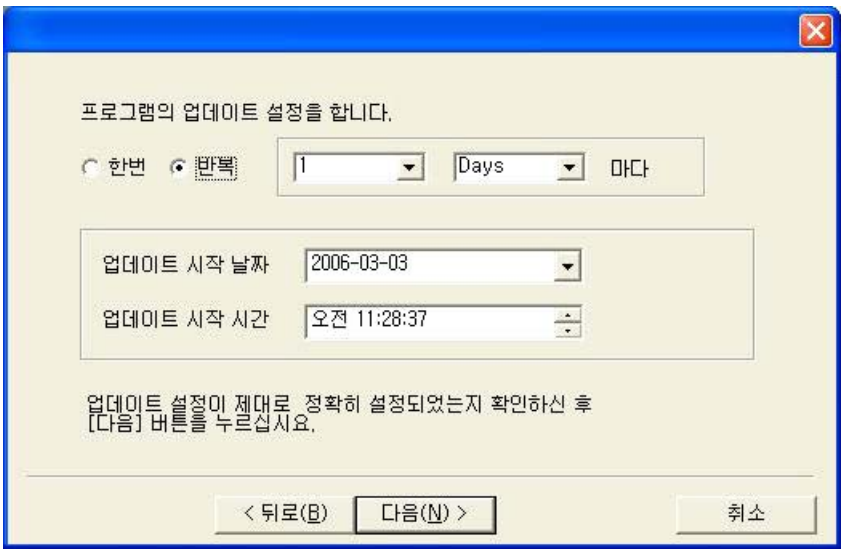
업데이트 스케줄 설정

[**변경**] 버튼을 클릭하면 업데이트 스케줄 정보 창이 활성화됩니다.



<그림48 업데이트 스케쥴 설정1>

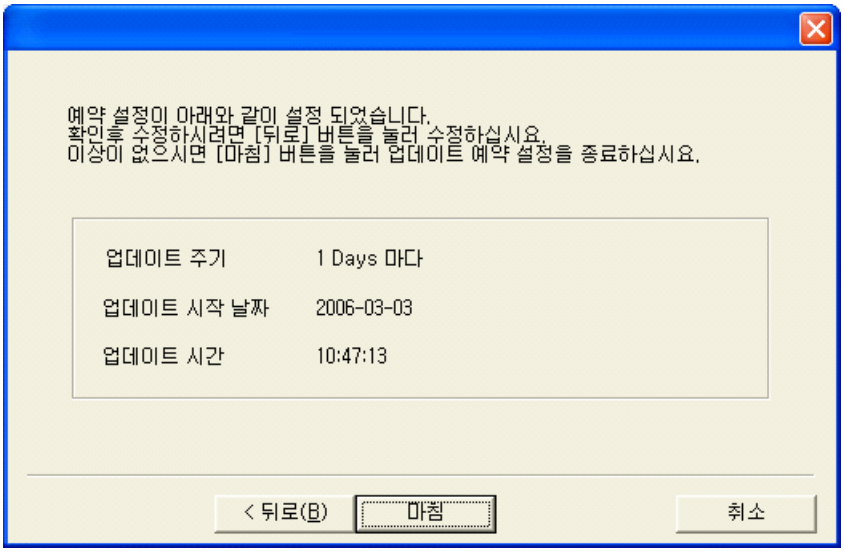
[**다음(N)**] 버튼을 클릭하면 다음과 같은 박스가 나타날 것입니다.



<그림49 업데이트 스케쥴 설정2>

이 박스에서는 해당 이벤트를 한번만 실행할 것인지 아니면 주기적으로 실행할 것인지를 결정합니다. "**한번**"만 선택한다면 이벤트를 지정한 시간에 한번 수행하지만 "**반복**"을 선택하면 지정한 시간부터 분, 시간, 요일 단위 등으로 주기적인 수행을 하게 됩니다. "**업데이트 시작 날짜**" 항목은 달력 프로그램으로 간편한 조정이 가능합니다. "**업데이트 시작 시간**" 은 시간, 분, 초 단위로 세밀하게 조정 가능합니다.

다음은 이벤트 설정 결과입니다.



<그림50 업데이트 스케쥴 설정3>

이벤트 설정을 마치고 나면 다음과 같이 표시될 것입니다.

<그림51 업데이트 설정>

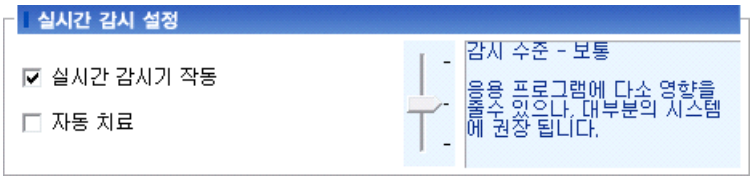
다음은 예약 설정기의 버튼 기능에 대한 것입니다.

[**수정**] 버튼
수정하고 싶은 이벤트를 클릭한 후 이 버튼을 클릭하면 해당 이벤트를 수정할 수 있습니다.

[**삭제**] 버튼
삭제하고 싶은 이벤트를 선택한 후 이 버튼을 클릭하면 해당 이벤트가 삭제됩니다.

실시간 감시 설정

이 설정에서는 스파이백신(SpyVaccine)의 실시간 감시기 작동 옵션을 지정할 수 있습니다.



<그림52 실시간 감시 설정>

실시간 감시기 작동

사용자가 직접 실시간 감시기를 설정하여 실시간으로 내부 또는 외부로부터 유입되는 악성코드를 차단하며, 최적화된 설계로 매우 적은 수준의 리소스를 점유하여 시스템에 무리를 주지 않고 악성코드를 진단할 수 있습니다.

<그림53 실시간 검사 리스트>

- 감시 수준 - 높음

  응용 프로그램 및 시스템의 성능에 영향을 미칠 수 있습니다. 인터넷 사용이 잦은 시스템에 권장됩니다.

- 감시 수준 - 보통

  응용 프로그램에 다소 영향을 줄 수 있으나, 대부분의 시스템에 권장됩니다.

- 감시 수준 - 낮음

  응용 프로그램 및 시스템 성능에 거의 영향을 주지 않습니다. 인터넷 사용이 낮은 시스템에 권장됩니다.

"감시수준 - 보통" 이 권장되는 옵션이며 감시 수준을 높여 파일을 실시간으로 모니터링 할 경우에는 시스템의 속도가 저하될 수 있습니다.

기타 설정

이 설정에서는 악성코드 치료 시 남기는 검사 기록파일을 생성 및 확인할 수 있고 "시스템 정리"에서 실수로 지울 수 있는 "즐겨 찾기" 항목을 저장 및 복원할 수 있습니다.

<그림54 기타 설정>

[보기]버튼은 "악성코드 검사 기록" 파일을 표시합니다. 날짜별로 기록된 내용을 분석하여 자신이 주로 감염되는 악성코드 내용을 확인할 수 있습니다.

<그림55 악성코드 검사 기록>

트리 항목을 마우스로 클릭하면 오른쪽 리스트 창에서 해당 일자에 검사 치료된 악성코드의 부가 정보가 표시됩니다. [인쇄] 버튼을 이용해 선택한 날짜의 해당 검사 치료 정보를 인쇄할 수 있습니다. 단, 컴퓨터에 프린트 기기가 설치되어 있어야 합니다.

예외 설정

악성코드 검사 시에 제외할 파일을 등록해 두면 악성코드 검사를 더욱 빨리 끝낼 수 있습니다. 단, 여기에 포함될 파일은 사용자가 악성 코드로부터 안전하다고 판단되는 것이어야 합니다.

<그림56 예외 설정>

설정 적용

고급 설정을 변경한 경우 반드시 설정적용 버튼을 클릭하여 변경된 옵션을 스파이백신에 적용시켜야 합니다.


EVERYZONE

6장

자주 질문되는 바이러스 Q&A

스파이백신(SpyVaccine) 사용자들이
자주 문의하는 질문들을 소개합니다.

Q : 악성 코드는 무엇입니까?

사용자의 의사와는 관계없이 시스템을 파괴하거나 정보를 유출하는 등 악의적 활동을 수행하도록 의도적으로 제작된 소프트웨어를 말합니다. 영어로는 "Malicious Software" 로 통상 "Malware"로 표현됩니다. 현재에는 바이러스(Virus) 및 인터넷 웜(Worm)과 트로이얀(Trojan), 백도어(Backdoor)를 지칭하는 해킹 툴, 악의적 스파이웨어, 애드웨어 등이 포함된 개념으로 이해되고 있습니다. 인터넷 웜과 더불어 가장 문제가 되고 있는 광고성 프로그램 등은 인증 받지 않은 Active-X 컨트롤을 통해 설치되거나 또는 신뢰할 수 없는 싸이트, 스팸 메일을 통해 사용자 모르게 설치되고 있습니다. 단순히 자주 방문 하는 싸이트를 알아보는 정보를 수집하는 것부터 시작하여 최근에는 수시로 뜨는 홍보용 광고성 팝업 창과 툴바, 시작페이지 강제 고정 등으로 발전하면서 사용자가 의도하지 않은 작용을 하게 되어 바이러스와 인터넷 웜 못지않은 파괴력과 위험성을 내포하게 되었습니다.

Q : 스파이 웨어는 무엇입니까?

Spyware 는 Aureate사의 Plugin 이며, 일반적으로 쉐어웨어 제작자가 소프트웨어를 무료로 제공하는 대가로 설치 이전에 사용자의 '동의'를 얻은 후에 프로그램 사용 시 사용자의 일부 정보(사용자의 동의를 얻은 정보)를 제공합니다. 설치 이전에 사용자의 동의를 얻고, 설치가 되기에 불법도 아니며, 감염을 시킨다거나 하는 바이러스 또는 자신을 널리 퍼뜨리는 웜도 아닙니다. 또한, 백도어나 트로이안 목마등도 아닙니다. 그러므로 터보백신 Ai 에서는 진단을 하되 삭제 기능을 제공하지 않고 있으며, 스파이웨어 전문 제거프로그램을 사용하셔야 합니다. 차후 Adware 프로그램의 설치 시 약관에 동의할 경우 어떤 정보가 제공되는지에 대해서는 유심히 살펴본 후에 동의를 한 후 설치하시기 바랍니다. 요즘은 사용자 약관이나 동의서들이 난무하는 관계로 안 읽고 지나치는 경우가 많이 있더군요. 귀찮더라도 조금씩 신경 쓴다면 차후에 발생하게 될 피해들을 미연에 방지할 수 있을 듯합니다. Spyware 기능이 포함된 소프트웨어 목록은 http://www.aureate.com/advertisers/network_members.html에서 보실 수 있습니다.

Q : 바이러스를 발견했습니다. 그런데 치료가 되지 않아요

대부분 진단과정에서 발견된 바이러스는 치료가 가능하지만 몇 가지 경우엔 안 됩니다. 첫째로 win/me 운영체제의 _Restore 폴더에 감염된 파일은 치료가 불가능합니다. 이 경우에는 저희 홈페이지 바이러스 FAQ 26 번을 참고해 주십시오. 두 번째는 환경설정의 문제입니다. 파일검사-> 모든 파일검사, 치료설정-> 파일삭제를 선택하시길 바랍니다. 세 번째는 윈도우즈의 시스템 폴더에 runonce.exe 파일이 없는 경우입니다. 이 경우는[재부팅 후 치료가 완료됩니다.]란 메시지가 나온 후 재부팅 후에도 치료가 안 되는 경우 입니다. 보통 runonce.exe 파일은 윈도우가 설치되면서 기본적으로 깔리는 파일이지만 가끔 없는 경우도 있습니다. 이 경우는 윈도우의 설치 cd를 이용하시거나 동일한 운영체제를 가진 컴퓨터에서 복사해 넣으시면 됩니다. 또한 타 백신의 시스템 감시기가 작동하는 경우에도 재부팅 시 치료가 되지 않습니다. 해당 백신 프로그램의 시스템 감시기를 잠시 사용 중지하신 다음 치료해 주십시오. 위의 경우가 아닌데도 치료가 안 된다면 사용하고 계시는 운영체제와 감염된 폴더, 그리고 치료 도중 오류가 나는 바이러스 이름을 적어서 다시 한 번 문의해 주시길 바랍니다.

Q : Windows XP 의 System Volume 에서 바이러스가 발견됩니다

Window XP 의 경우는 시스템 복원 기능이 있어서 시스템에 문제가 생길 경우 간단하게 이전의 상태로 복원 시킬 수가 있습니다. 시스템을 복구하는데 필요한 파일은 C:₩System Volume Information₩_restore 폴더에 있습니다. 이 폴더는 숨김 속성의 폴더로 문제가 생기기 바로 이전의 시스템에서 사용된 파일을 저장하고 있습니다. 만약 바이러스가 windows XP 의 어떤 파일이 감염되어 치료했다면 이 폴더에는 치료하기 이전의 파일이 들어가게 됩니다. 즉 시스템 복구를 위해 저장된 파일이 실상은 감염된 파일인거죠. 그래서 백신으로 검사는 되지만 치료불가인 것은 이 폴더의 내용을 마음대로 사용할 수가 없기 때문입니다. 치료 방법은 운영체제의 특성상 windows XP의 시스템 복구 기능을 제거하기만 하면 됩니다. C:₩System Volume Information₩_restore에 감염되어있는 바이러스는 컴퓨터에 영향을 미치지 않습니다. 그래도 사용자님께서 불안하시다면 위에서 말씀드린 대로 복원 기능을 사용하지 않기를 바랍니다. 그러면 다음 부팅 때는 C:₩System Volume Information ₩_restore 폴더에 백업된 내용이 자동적으로 삭제됩니다.
시스템 복원(즉, restorept.api)은 "마지막으로 성공한 구성"과 비슷한 Windows XP 의 새로운 기능이다. 시스템 복원은 하나가 아닌 여러 개의 복원 시점(point)들을 유지할 수 있다. 사용자는 수동으로 복원 시점을 생성할 수 있고 또한 다음과 같은 과정을 통해 복원 시점을 유지할 수도 있다.

1. 새로운 소프트웨어 설치(만약 현재 installer를 사용하는 애플리케이션이 시스템 복원과 호환된다면)
2. AutoUpdate 사용
3. 복원 작업 수행 중
4. 마이크로소프트 백업 또는 복구 작업
5. 서명되지 않은 드라이버의 설치
6. 24시간 동안 아무런 동작이 없을 때 자동으로

기본적으로 시스템 복원은 모든 파티션을 모니터링한다. 그래서 예를 들면, 사용자가 실행파일을 지운다면 나중에 시스템 상태가 특정한 파일의 상태를 되돌릴 수 있다. 사용자가 복원시점으로 되돌릴 때, 그 시점 이후의 모든 변경사항들을 잃게 된다. 단, My Documents 폴더와 사용자가 생성한 워드나 액셀과 같은 문서는 예외이다.
만약 시스템 복원을 사용하고 새로운 시스템 상태가 맘에 들지 않는다면, 이전에 시스템 복원을 수행했던 시점으로 시스템을 되돌릴 수 있다. 다른 방법으로는 다양한 복원 시점으로 시스템 상태를 되돌리기 위해 시스템 복원(System Restore)을 사용할 수도 있다.

시스템 복원을 사용 또는 사용하지 않는 방법

1. 제어판에서 시스템을 실행한다.(시작 -> 설정 -> 제어판 -> 시스템)
2. System Restore 탭을 선택한다.
3. 시스템 복원 기능을 사용하려면 "Turn off System Restore on all drives" 를 체크 해제한다. 반대도 가능하다.
4. OK를 클릭한다.

또한 Settings 버튼을 클릭하여 복원 정보에 사용하기 위한 각 드라이브의 최대용량을 설정할 수 있다. 만약 사용자가 선택한 드라이브가 시스템 드라이브가 아니라면, 사용자는 각 드라이브 별로 시스템 복원 기능을 사용하지 않게 할 수 있다. 최대 용량은 드라이브 당 12% 이다.

레지스트리를 수정하는 방법

1. 레지스트리 편집기를 시작한다 (시작 -> 실행 -> regedit.exe 입력)
2. HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩SystemRestore로 이동한다. 만약 DisableSR이 없다면 DWORD값으로 생성한다.
3. 값을 1로 하면 시스템 복원을 사용하지 않게 되고, 사용하려면 0으로 세팅한다.
4. HKEY_LOCALMACHINE₩SYSTEM₩CurrentControlSet₩Services₩sr로 이동한다
5. 시스템 복원 서비스가 부팅 시 시작되지 않도록 하기 위해 Start 값을 4로 시작 시 실행되게 하려면 0으로 세팅한다.
6. 레지스트리 편집기를 닫는다.

Q : Windows ME 에서 _Restore 폴더에 바이러스가 감염되었습니다

Windows ME의 경우는 시스템 복원 기능이 있어서 시스템에 문제가 생길 경우 간단하게 이전의 상태로 복원 시킬 수가 있습니다. 매우 편리한 기능입니다. 시스템을 복구하는데 필요한 파일은 C:₩_Restore 폴더에 있습니다. 이 폴더는 숨김 속성의 폴더로 문제가 생기기 바로 이전의 시스템에서 사용된 파일을 저장하고 있습니다. 만약 바이러스가 Win/ME의 어떤 파일이 감염되어 치료했다면 이 폴더에는 치료하기 이전의 파일이 들어가게 됩니다. 즉 시스템 복구를 위해 저장된 파일이 실상은 감염된 파일인거죠. 그래서 백신으로 검사는 되지만 치료불가인 것은 이 폴더의 내용을 마음대로 사용할 수가 없기 때문입니다. 치료 방법은 운영체제의 특성상 Win/ME의 시스템 복구 기능을 제거하기만 하면 됩니다. C:₩_Restore에 감염되어 있는 바이러스는 컴퓨터에 영향을 미치지 않습니다. 그래도 사용자님께서 불안하시다면 위에서 말씀 드린 대로 복원기능을 사용하지 않기를 바랍니다. 그러면 다음 부팅 때는 C:₩_Restore 폴더에 백업된 내용이 자동적으로 삭제됩니다.

시스템 복원 제거 방법

1. "시작->제어판->시스템" 에서 "성능"탭을 클릭
2. "파일시스템" 메뉴->"문제 해결" 탭 클릭
3. "시스템 복원 사용 안함" 을 선택 후
4. 재시작 하셔야 합니다.

위의 방법으로 안되면 바이러스가 어느 폴더에 있는 지 확인한 후 도스 부팅 디스켓으로 부팅한 후 "_Restore"로 간 후 바이러스가 있는 폴더로 간 후 지우시면 됩니다. (예를 들어 "temp" 폴더 안에 바이러스가 있으면 "cd temp"를 하고 Enter 키를 치신 후 del 명령으로 모든 파일을 지우면 됩니다. "dir" 명령을 치시면 파일을 볼 수 있습니다. 숨김 속성이 있는 파일은 "dir /ah"를 하셔야 보실 수 있습니다.)

Q : 검색 도중에 컴퓨터가 멈춥니다

하드디스크에 배드 섹터와 같은 에러가 많을 경우 발생하는 에러입니다. 이 경우는 시작 -> 프로그램 -> 보조 프로그램 -> 시스템 도구의 시스템 검사를 먼저 실행해 디스크 에러를 먼저 해결하셔야 합니다.

Q : 닫기 창과 아이콘이 이상한 숫자로 변했어요. 바이러스 인가요?

이 문제는 크게 두 가지로 나눌 수가 있습니다.
첫째는 메모리와 관련 되서 나타나는 현상일 수 있고, 둘째는 windows의 다국어 지원에 관련된 font 이상 현상일 수 있습니다.

우선 다음과 같은 조치를 취해주시기 바랍니다.

1. 먼저 시스템을 정상 종료 합니다.
   정상종료 : [시작]-[시스템 종료]-[시스템 재시작]
2. 다시 부팅할 때 F8을 눌러 부팅 메뉴를 나타나게 합니다.
3. 여기서 safe mode를 선택합니다.
4. safe mode로 window를 가동한 후에는 다시 정상 종료를 합니다.
5. 재부팅 후에 문제가 해결 되었는지 확인합니다.

이 방법으로 해결이 안 되는 경우는 다음을 따르시기 바랍니다.

1. [제어판]->[프로그램 추가/삭제]를 선택
2. window 설치 탭을 클릭
3. 구성요소에서 "다국어 지원" 란에 체크 표시가 되어 있는지 확인
   체크 표시가 되어 있지 않다면 체크합니다.
4. [확인]을 클릭하신 후 window CD를 씨디롬에 넣고 [확인]을 클릭
5. 파일 복사를 끝내면 시스템을 다시 재부팅
6. 재부팅 후에 문제가 해결되었는지 확인하십시오.

Q : 바이러스 치료 후 하드 디스크 용량이 줄어들었습니다

만약 치료된 파일의 용량이 100M 라면 100M의 백업 파일이 생성될 것입니다. 이는 터보백신의 치료 설정에서 "치료 시 이전 파일 보관" 옵션에 체크를 했을 경우 생깁니다. 백업된 파일은 치료 시 손상 등의 만약의 사태에 대비해서 보관되는 파일이며, 일반적으로 바이러스 치료 후에는 필요 없는 파일입니다. 백업 파일 복원기를 이용하여 모두 선택한 후에 삭제를 해주시면 백업파일이 제거될 것입니다.

Q : 인터넷이 느려졌습니다

인터넷 홈페이지 상에서 입력 창에 글을 쓸 때 느려지는 것은 인터넷 익스플로러 상에서 [도구]->[인터넷 옵션]->[내용]->["개인 정보" 중 "자동 완성"]->["자동 완성 사용 대상" 중 "양식의 사용자 이름과 암호"] 항목의 체크를 해제해주시면 답답함을 덜 수 있습니다. 또 다른 원인으로는 W95/CIH 바이러스 등에 의해 윈도우의 일부 파일이 손상된 경우입니다. C:₩Windows₩system 폴더내의 "Pstores.exe" 파일이 손상된 경우 인터넷이 현저하게 느려질 수 있습니다. 이런 경우에는 시스템 파일 복구를 사용해 보시기 바랍니다. 또는 동일한 운영체제를 쓰는 정상적인 컴퓨터에서 복사하여 덮어씌우십시오.

시스템 파일 복구법

운영체제 CD를 넣으신 후, [시작]->[실행]에서 SFC라 입력하신 후 메시지에 따라 진행하시기 바랍니다.

Q : 인터넷 익스플로러에서 한글 입력이 안됩니다

이 방법은 마이크로소프트에 가서 검색하시면 나옵니다.
다음과 같은 방법으로 해보세요.

1. Ctfmon.exe 파일을 지워야 됩니다.
   시작 -> 실행
   Regsvr32.exe /u msimtf.dll -> 메세지가 나오면-> 확인-> 엔터
   Regsvr32.exe /u msctf.dll -> 메세지가 나오면 -> 확인 -> 엔터
   위와 같이 하면
   ctfmon.exe의 실행을 유도하는 두개의 dll 파일이 제거 됨.

   시작->실행->regedit
   HKEY_CURRENT_USER->Software->Microsoft->Windows->CurrentVersion->Run에서, ctfmon.exe을 삭제

ctfmon.exe를 지워도 한글입력에는 아무런 문제가 발생되지 않습니다.
ctfmon.exe의 자세한 내용은 아래사이트에서 검색 해보세요.

출처 : 마이크로 소프트 - KR282599문서 참조

2. 레지스트리 편집 창으로 가서 HKEY_ LOCAL _ MACHINE → Software → Microsoft → Windows → Current Version → Network → Real Mode Net 항목의 오른쪽 창에서 Autologon 항목을 삭제하고 재부팅

Q : 인터넷 익스플로러가 느려질 때

본 내용은 인터넷 익스플로러가 늦게 뜨거나 [오류보고] 가 인터넷 익스플로러 실행 시 부터 계속 발생하는 경우에 해당되며, 사용 중에 가끔 발생하는 경우는 해당되지 않습니다.

DigitalNames가 설치된 경우

DigitalNames 라는 한글 도메인 유틸리티의 오류 문제일수 있습니다.
정확한 원인은 밝혀지지 않았지만 DigitalNames를 제거하고 나서는 오류보고 문제가 발생하지 않는 경우가 많았습니다. 제거하기 위해서는 아래 제거 방법을 참고하시기 바랍니다.

DigitalNames 제거방법

윈도우즈 시스템 폴더에 있는 DigitalNameUninstall.exe 프로그램을 실행해서 제거합니다. (없는 경우는 DigitalNames가 설치되지 않은 경우이므로 해당되지 않습니다.)
윈도우즈 시스템 폴더 (Win9x - C:₩Windows₩System, WinNT/2000 - C:₩WinNT₩System32, WinXP - C:₩Windows₩System32)

DigitalNames가 설치되어 있지 않은 경우

요즘 발생하는 바이러스중의 일부는 BHO(Browser Helper Object)로 동작하는 방법으로 인터넷 익스플로러에 포함되어 같이 실행되도록 합니다. 이 때문에 인터넷 익스플로러나 윈도우즈 탐색기 실행 시 프로세스를 거의 100%씩 차지하면서 늦게 실행되는 경우가 발생하거나 아예 인터넷 익스플로러 또는 제어판 실행시 [**오류보고 - 보냄, 보내지 않음**]을 발생하기도 합니다. 이런 경우에는 [시작]->[실행]-> regedit를 실행해서 아래의 레지스트리 키 밑에 있는 서브 키들을 삭제해 주시기 바랍니다.
서브키 예) {137200AB-4B41-4ACF-942A-B053BFE30038}

HKEY_LOCAL_MACHINE₩Software₩Microsoft₩Windows₩CurrentVersion₩explorer₩Browser Helper Objects

단, 자신이 사용하고 있는 프로그램의 모듈이 포함되어 있을 수도 있으므로 삭제하기 전에 어떤 모듈인지 먼저 확인하시고 필요한 모듈이라면 삭제하지 마시기 바랍니다. (좋은 방법으로는 하나씩 지워가면서 인터넷 익스플로러를 실행해 보는 것입니다.)

Q : 특정 싸이트에 접속하면 여러 개의 창이 연속으로 뜹니다. 바이러스입니까?

우선 바이러스에 의한 영향이 아님을 밝혀 둡니다. 연속적으로 원치 않는 창이 계속 뜨는 경우는 외국의 싸이트에서 자주 발생 합니다. 때문에 짜증이 이만저만 한 것이 아닙니다. 이 경우 보통 다운될 지경까지 이르고 마는데 그 전에 Ctrl + Alt + Del 로 프로그램 작업 리스트를 띄우신 후, 익스플로러 자체를 없애셔도 됩니다. 또는 부모 창(제일 처음 뜨던 창)을 없애주시면 나머지 창이 계속 발생하는 것을 막을 수 있습니다. 그런 후 스파이웨어 전문 제거 툴을 사용하여 애드웨어 프로그램이 설치되 있는 것은 아닌지 진단해 보시기 바랍니다.

Q : 스파이웨어 제거프로그램을 사용하지만 자주 감염이 일어납니다

p2p 프로그램을 사용하시면 부가적으로 설치되는 애드웨어 중에 다음 항목을 살펴보시고 제거해 보시기 바랍니다. [제어판]->프로그램 추가 삭제 에서 다음 프로그램을 제거해 주십시오.

1. Reg2
2. Error Search Assistant Reset"
3. Search Button Reset"
4. Search Assistant Reset"
5. Web Contextual Reset"
6. WebRebates (by TopRebates.com)
7. WinTools Easy Installer
8. WinTools for Internet Explorer [v2]
9. Win-Tools Easy Installer (by WebSearch)
10. Search Assistant - My Search
11. Search Assistant Uninstall
12. Search Assistant
13. WebSearch Tools
14. ISTsvc
15. SlotchBar
16. WebRebates (by TopRebates.com)
17. EliteBar Internet Explorer Toolbar

단, WinTools for Internet Explorer 프로그램을 제거할 때는 ''N''->''N''->''Y'의 순서로 물음에 답해야만 제거가 됩니다.

Q : 컴퓨터 부팅 시 이상한 소리가 납니다

컴퓨터 바이러스 중 W95/LOVE라는 바이러스는 매월 1일 귀에 익숙한 LG 로고송을 내 보냅니다. 이런 경우는 부팅 후 터보백신을 이용하여 치료할 수 있습니다만 그런 현상이 아닌 경우에는 대부분 메인보드의 하드웨어 모니터링 센서에서 비정상적인 문제로 인해 그런 현상이 발생하는 경우가 많습니다. 쿨링팬이 작동을 멈췄다든지, CPU온도가 비정상적으로 높다든지, CPU온도제어 관련 프로그램을 잘못 설치했다든지 하면 삐~ 하는 경고음을 내게 됩니다. 어느 정도 컴퓨터를 다룰 줄 아신다면 그 원인을 찾아내실 순 있습니다만, 심각한 경우는 메인보드에 문제가 발생했을 가능성도 있습니다. 이런 경우는 메인보드 수리가 필요하며 계속적인 문제로 인해 사용에 지장이 있으시면 AS를 요청해 보시기 바랍니다.

Q : 특정 싸이트만 접속이 되지 않습니다. 바이러스 인가요?

네트워크 환경 등록 정보의 [설치된 네트워크 구성요소]항목을 모두 삭제하신 다음 재부팅한 후에 다시 설치하면 해결될 것입니다.

Q : Trojan.. 어쩌구 하는 것에 감염되어서 치료했는데 어떤 바이러스 인가요?

일반적으로 백오리피스, 백도어 등을 포괄해서 일반적으로 불리는 말이지만 약간의 개념차이는 존재합니다. 어찌됐든 Trojan(백오리피스, 백도어)는 윈도우의 TCP/IP 기능을 이용하여 시스템끼리 원격 제어가 가능하므로 멀리 떨어진 컴퓨터의 데이터를 사용자의 허락없이 임의대로 조작(파일 삭제·복사·이동, 파일 또는 디렉토리 찾기, 디렉토리 생성·삭제, 파일 압축과 압축 해제 등)할 수 있는 악성 바이러스에서부터 상대방의 컴퓨터에 잠입했다가 일정시간이 지나면 파일을 지우던가 그림을 띄우는 등 여러 가지 변형된 형태가 있습니다. 또한, 시스템 정보를 얻을 수 있는 것은 물론, 사용자가 입력하는 내용이나 암호를 몰래 카메라처럼 갈무리하거나 해당 내용을 파일로 저장했다가 다른 사람의 컴퓨터로 빼돌릴 수도 있으며, 컴퓨터를 재부팅 시킬 수도 있습니다. 이러한 종류들은 바이러스처럼 자신을 복제하는 기능은 없지만 악용될 경우 피해가 우려되어 진단이 되는 즉시, 삭제 하셔야 합니다. 파일들을 겹쳐 쓰거나 붙어서 기생하는 경우가 아니기 때문에 단순히 해당 파일을 삭제하는 것으로 치료가 가능합니다. 단, 이 프로그램은 사용자 모르게 시스템에서 이미 실행 중인 경우가 많으므로 삭제가 안 되어 Dos모드로 들어가 치료하는 경우도 있습니다.


EVERYZONE