



Virus Chaser

Beyond Tradition

본 소프트웨어 제품 및 소프트웨어의 복사본들에 대한 지적 재산권을 포함한 일체의 권리는 에스지에이㈜가 소유합니다. 이권리는 대한민국의 저작권법과 국제 저작권 조약으로 보호 받습니다.

Copyright © SGA Co.,Ltd. All rights reserved.



KOSDAQ
코스닥상장법인



시스템요구사항

소프트웨어 환경_Windows 32bit, 64bit 모두 지원

- 2000 Professional
- XP Home Edition
- XP Professional
- Vista
- 7 Home Premium
- 7 Professional
- 7 Ultimate
- 8
- 8 Professional

- 2000 Server
- Server 2003
- Server 2003(R2)
- Server 2008
- Server 2008 R2
- Server 2012

하드웨어 환경

- CPU : Intel Pentium 1GHz 이상 IBM 호환 기종
- Memory : 512MB 이상(1GB 이상권장)
- HDD : 500MB 이상의 여유공간

137-896 서울시 서초구 마방로2길 44(양재동 315-1) 대표전화: 070-7308-1004
팩스: 02-575-1807 구매문의: sales@sgacorp.kr URL: http://www.viruschaser.com
@virus_chaser http://www.facebook.com/viruschasercorp

Security Global Alliance



바이러스체이서 8.0 사용설명서

CONTENTS

01	개요	3
02	특징	3
03	주요기능	3~4
04	설치	5~8
	4.1. 설치 전 확인사항	5
	4.2. 시스템 요구사항	5
	4.3. 설치과정	6~8
05	사용설명	8~18
	5.1. 프로그램 실행	8~9
	5.2. 메인 프로그램	9~18
06	제거	18
07	고객지원	19

1.개요

‘바이러스체이서 8.0’은 급변하는 IT환경에 맞춰 점차 다양하고 지능적으로 변하는 여러 보안 위협에 대비하기 위해 개발된 **스스로 알아서 신/변종 악성 코드의 실행을 차단**하는 신개념 통합안티바이러스 제품입니다. 특허를 취득한 ‘악성 프로세스의 행위를 기반으로 한 악성코드 차단기술’이 적용된 프로액티브(Proactive)방식의 **BODAR(Behavior Oriented Detection At Run-time)** 엔진을 탑재하여 악성 프로세스의 행위를 실시간으로 지켜 “보다”라는 의미로 타사의 패턴 시그니처 기반의 엔진 “보다”뛰어난 실시간 엔진을 탑재하여 APT(Advanced Persistent Threat) 공격에 “보다”효과적으로 대응이 가능합니다. CC(Common Criteria)인증으로 **보안성**을, 특허 획득으로 **기술력**을, GS인증으로 **품질성**을 인정받은 ‘바이러스체이서 8.0’이 신/변종 악성코드의 피해로부터 사용자의 컴퓨터를 안전하게 보호할 것입니다.

2.특징

- 차세대 프로액티브 방식의 BODAR(Behavior Oriented Detection At Run-Time)(행위기반 탐지/차단) 엔진 탑재
- 스스로 알아서 신/변종 악성코드의 실행을 차단
- **Strong**(높은 바이러스 검출율), **Speed**(더욱 빨라진 검사속도), **Simple**(쉽고 간편한 기능), **Small**(최저 리소스 유지)

3.주요기능



행위기반 탐지/차단

악성코드 발견 시 패턴 업데이트 후 처리되던 기존 방식이 아닌 별도의 패턴 업데이트 없이 악성코드가 실행 시 행위를 감시하여 악성 행위가 발견되면 실시간으로 차단합니다.



실시간 감시

악성코드가 수행될 때 자동 치료 또는 사용자가 응답 할 때까지 관련 악성코드가 동작하지 못하도록 잡아두어 어떠한 경우에도 바이러스가 실행되어 컴퓨터에 피해를 입히는 것을 방지할 수 있습니다.
(실시간 감시는 1차적으로 행위기반으로 감시하고 2차적으로 패턴 시그니처 기반으로 악성코드를 비교 합니다.)



자체 보호기능

바이러스체이서와 시스템 파일의 변조를 방지하여 컴퓨터가 안전한 상태로 유지될 수 있도록 합니다.



패턴 시그니처 기반 탐지

최소의 패턴으로 매우 복잡한 악성코드를 깊고 섬세하게 검출 할 수 있습니다.

■ 시그니처 기반

바이러스 샘플을 기반으로 패턴을 가지고 진단을 하는 백신을 총칭.



빠른 검사 속도

각 O/S 또는 기업에 알맞은 검사 후 기존 파일을 재 검사 안해도 정상파일로 확인하여 검사 속도를 빠르게 향상시키며, 오진을 방지 할 수 있는 기능이 포함되어 있습니다.



가벼운 실행

설치 용량 70MB 이하로 시스템을 감시하며, 가볍게 동작하므로 백신의 설치 전 사용자가 느끼는 체감 속도를 그대로 유지 할 수 있습니다.



간편한 환경설정

기본적인 기능을 모두 포함하면서도 설정이 반드시 필요한 최소한의 주요 기능만을 환경 설정 메뉴로 채택하였고, 사용자가 설정하기 어려운 부분은 학습이 가능한 인공지능 기능으로 처리하여 사용이 간편 합니다.

SGA Security Center 'SGA-SC2.1' 통합보안관리 솔루션 (중앙관리 시스템)



통합보안관리 솔루션 (중앙관리 시스템)

바이러스체이서의 중앙 관리뿐만 아니라 PMS (Patch Management System)으로 확장이 가능한 중앙 관리 도구를 제공 합니다.

4. 설치

4.1. 설치 전 확인 사항

바이러스체이서 8.0은 기업용, 개인용, 그리고 특화된 기업용 설치 파일로 구분되며 만약, 인터넷에 연결되지 않은 네트워크에 설치 할 경우 공급업체와 사전 협의가 필요합니다. 또한 설치하기 전에 다음 사항을 확인해야 합니다.

1) 바이러스체이서 8.0은 시스템의 중요한 부분을 직접 감시하는 안티 바이러스 제품이므로 비슷한 유형의 안티 바이러스 제품이 이미 설치되어 있는 경우 반드시 타 제품을 제거하고 설치해야 합니다.

2) 바이러스체이서 8.0이 지원하는 O/S는 다음과 같습니다. **(4.2 시스템 요구 사항 참조)** 이들 제품 외에는 설치가 되지 않거나 설치 되어도 이상 현상이 발생 될 수 있습니다.

단, 각 O/S별 서비스 팩에 관계없이 모두 설치가 가능합니다.

3) 시스템과 밀접한 관련이 있는 특정 소프트웨어와 충돌 가능성이 있으므로 프로그램 디버그 등 분석과 관련된 소프트웨어가 설치된 컴퓨터에는 설치하지 않는 것이 좋습니다.

4.2. 시스템 요구 사항

하드웨어 환경

- CPU : Intel Pentium 1GHz 이상 IBM 호환 기준
- Memory : 512MB 이상(1GB 이상권장)
- HDD : 500MB 이상의 여유공간

지원언어

- 한글
- 영어
- 일본어

웹브라우저

- Microsoft Internet Explorer 5.0 이상
- 인터넷연결(데이터베이스 및 애플리케이션 모듈 업데이트를 위해 필요)

소프트웨어 환경 - 32bit, 64bit 모두 지원

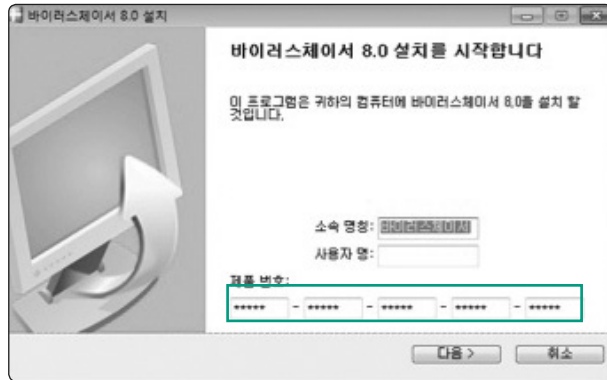
Windows 2000 Professional	
Windows XP Home Edition	
Windows XP Professional	
Windows Vista	Windows Server 2000
Windows 7 Home Premium	Windows Server 2003
Windows 7 Professional	Windows Server 2003 (R2)
Windows 7 Ultimate	Windows Server 2008
Windows 8	Windows Server 2008 R2
Windows 8 Professional	Windows Server 2012

4.3. 설치 과정

바이러스체이서 8.0의 설치 과정은 쉽고 간단합니다. 아래의 내용은 개인용 바이러스체이서 8.0에 대한 것입니다. 기업의 경우 이미 설치되어 있는 관리 툴 등을 이용하여 다양한 방법으로 설치가 가능하며 구체적인 내용은 공급업체와 상의 하는 것이 좋습니다.

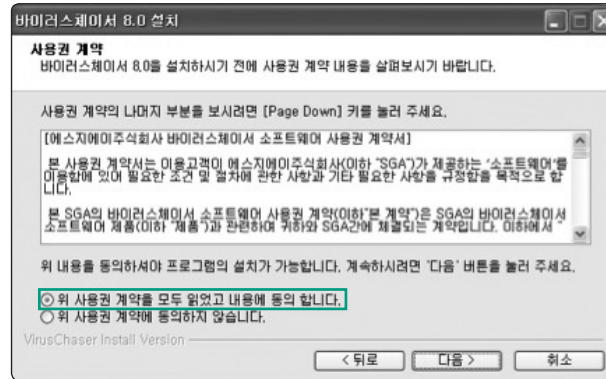
1) 설치 시작

설치 파일 이름은 일반적으로 Setup.exe라는 이름으로 되어 있고, 실행을 시키면 다음과 같이 나타납니다. 이때, 제품 구입 시 함께 받은 제품 번호와 소속 명칭, 사용자 명을 입력하고 “다음” 버튼을 누릅니다.



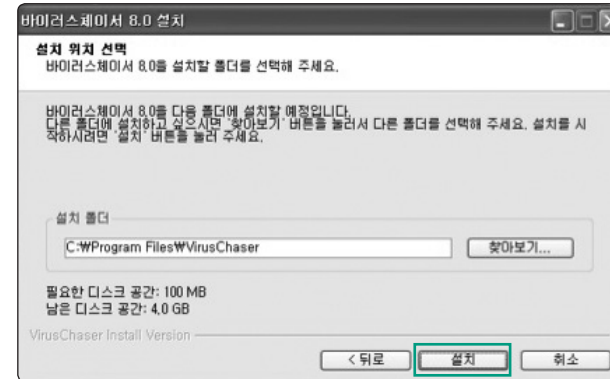
2) 사용권 계약과 동의

다음과 같이 사용권 계약에 동의를 해야 설치가 가능하며 계약의 내용을 잘 읽은 후 “위 사용권 계약을 모두 읽었고 내용에 동의 합니다.”를 선택하고 “다음” 버튼을 누릅니다. 단체사용자의 경우 별도의 사용권 계약이 이루어지고 이런 과정들이 모두 생략됩니다.



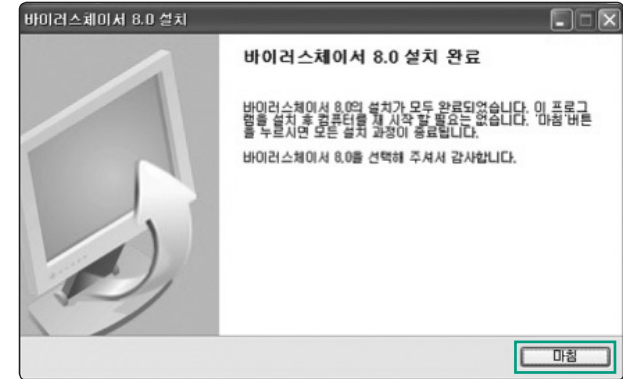
3) 설치 경로 선택

바이러스체이서 8.0을 설치 할 폴더를 선택 할 수 있으며, 일반적으로는 운영체제가 설치된 드라이브의 “Program Files\VirusChaser”에 설치 됩니다. “설치” 버튼을 누르면 설치가 시작됩니다. 설치에 소요되는 시간은 환경에 따라 다소 차이가 있지만, 평균적으로 약 2~3분 정도 소요됩니다.



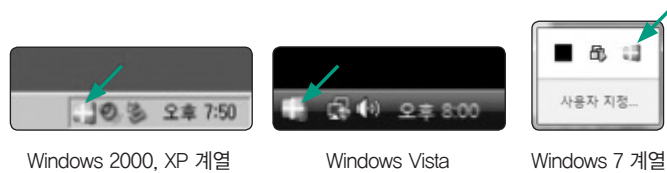
4) 설치 완료

설치가 완료되면 다음과 같은 화면이 나타나고 “마침” 버튼을 누르면 모든 설치 과정이 종료됩니다.



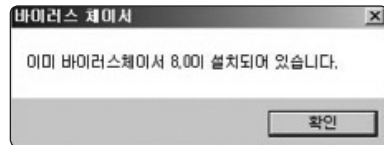
5) 설치 확인

설치가 완료되면 다음과 같은 트레이 아이콘이 표시됩니다.
재 시작 할 필요는 없지만 본 제품이 설치 되기 전에 이미 바이러스에 감염된 컴퓨터의 경우 설치 후 컴퓨터를 재 시작해야 안정적으로 사용 할 수 있습니다.



6) 설치 실패

바이러스체이서 8.0이 이미 설치되어 있는 경우 설치를 진행 할 수 없습니다.



부득이 재 설치를 해야 한다면, 이미 설치 된 바이러스체이서 8.0을 제거 후 설치 해야 합니다. (“6. 제거” 항목 참조)

7) 설치 주의 사항

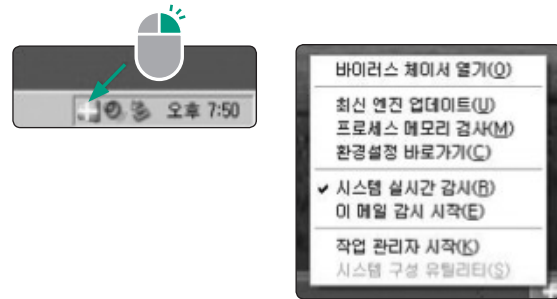
바이러스체이서 8.0 설치 시 바이러스체이서 8.0 이전 버전이 설치되어 있으면 자동으로 제거합니다.

5.사용설명

5.1. 프로그램 실행

바이러스체이서 8.0이 설치되면 자동으로 프로그램이 실행되어 시스템을 보호하게 됩니다.

바이러스체이서 8.0의 관리 콘솔을 실행시키기 위해서는 다음과 같이 트레이 아이콘에 마우스 오른쪽 버튼을 클릭하고 “바이러스체이서열기”를 선택합니다.



■ 바이러스체이서 열기

– 관리 콘솔을 실행시킵니다.

■ 최신 엔진 업데이트

– 업데이트 서버로부터 최신 엔진을 받아옵니다.

■ 환경설정 바로 가기

– 환경설정 메뉴를 실행시킵니다.

■ 프로세스 메모리 검사

– 현재 실행중인 프로세스 및 관련 모듈에 대해 바이러스 검사를 실시합니다

■ 시스템 감시 일시 중지

– 시스템 감시를 일시적으로 중지시키거나 실행합니다.

■ 이 메일 감시 시작

– 이 메일 감시를 시작하거나 종료시킵니다.

■ 작업 관리자 시작

– 윈도우즈 시스템의 작업 관리자를 실행시킵니다.

■ 시스템 구성 유틸리티

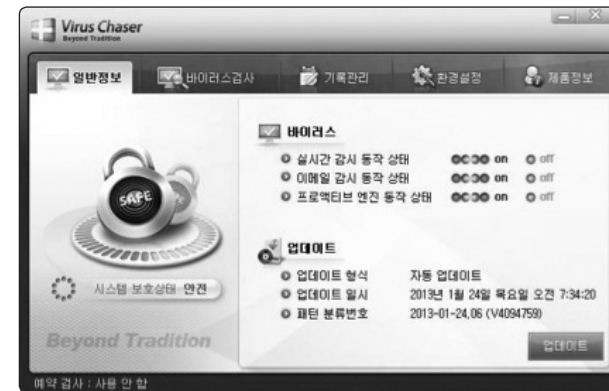
– 시스템 구성 유틸리티가 실행됩니다.
(비활성화 되어 있으며 Ctrl+Shift 키를 누른 상태에서 클릭하면 활성화 됩니다.)

5.2. 메인 프로그램

메인 프로그램은 실행 시 가장 먼저 일반정보 메뉴가 표시되며 바이러스검사, 기록관리, 환경설정, 제품정보로 구성되어 있습니다.
특정 메뉴로 이동을 원할 경우 상단에 나열 된 탭을 선택하면 됩니다.

■ 일반 정보

바이러스체이서 8.0의 현재 상태를 요약해서 표시해주며 실시간 감시 동작 상태, 이메일 감시 동작 상태, 예약검사, 업데이트 형식, 업데이트 일시(최신 패턴 버전으로 업데이트가 된 일시), 패턴 분류번호 등의 정보를 확인할 수 있습니다.



■ “업데이트” 버튼

일반정보 탭에서 업데이트 버튼을 누르면 최신 패탄을 업데이트 할 수 있습니다.
(트레이 아이콘 메뉴의 “최신 엔진 업데이트”와 동일)



■ 바이러스 검사

바이러스 검사와 관련한 설정 및 검사 실시, 불필요 항목 삭제 기능을 제공 합니다.

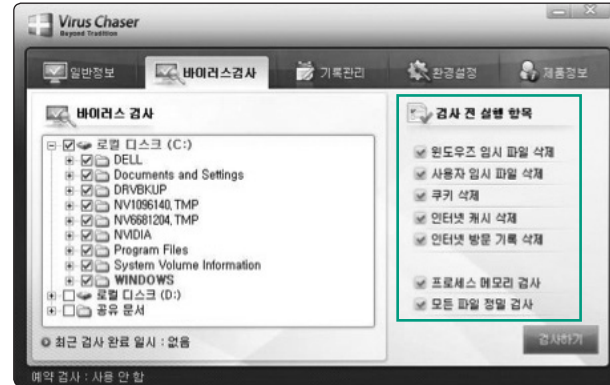


• 바이러스 검사(좌)

메뉴의 설정에 따라 디스크 전체 혹은 검사대상 폴더 설정 필드에서 검사할 폴더에 체크하여 검사를 수행 합니다.

■ 바이러스 검사

바이러스 검사와 관련한 설정 및 검사, 불필요 항목 삭제 기능을 제공합니다.



• 검사 전 실행 항목(우)

검사 전 실행 항목 선택에 따라 시스템에 존재하는 윈도우 임시 파일, 사용자 임시 파일 등을 정리하여 시스템을 최적화할 수 있습니다.

바이러스 검사 전 체크 된 항목의 내용을 수행 합니다.

“프로세스 메모리 검사” 체크를 하면 전체 검사를 수행 하기 전에 현재 실행되고 있는 프로세스에 대해 바이러스 검사를 실행합니다.

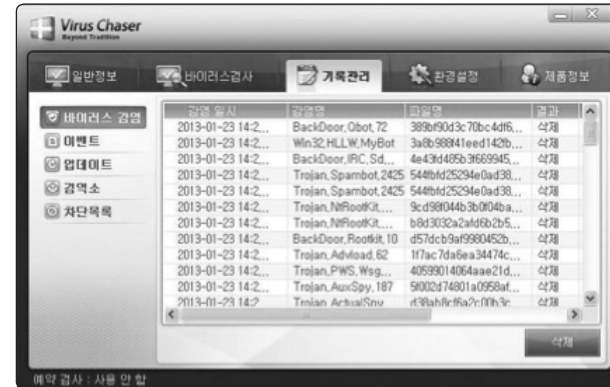
“모든 파일 정밀 검사” 체크를 하면 모든 파일에 대해 정밀검사를 실행 합니다.
(체크하지 않을 경우 : “exe,com,bat,doc,ppt,xls,inf,vbs,vbe” 확장자만 검출합니다)

■ 기록관리

바이러스체이서 8.0에서 발생한 다양한 로그를 확인할 수 있습니다.

• 바이러스 감염

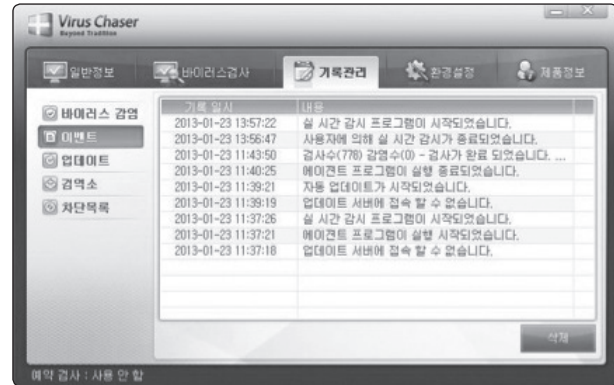
시스템에서 검출된 바이러스에 대한 기록을 열람할 수 있습니다.



항 목	내 용
감염일시	바이러스 검출 일시
감 염 명	바이러스 명(진단명)
파 일 명	바이러스로 검출 된 파일명
결 과	바이러스 처리 결과(치료/삭제/무시)
검사방법	바이러스를 검출 한 경위(수동/자동 검사, 실시간 감시)
파일경로	바이러스가 검출 된 저장소의 경로

• 이벤트

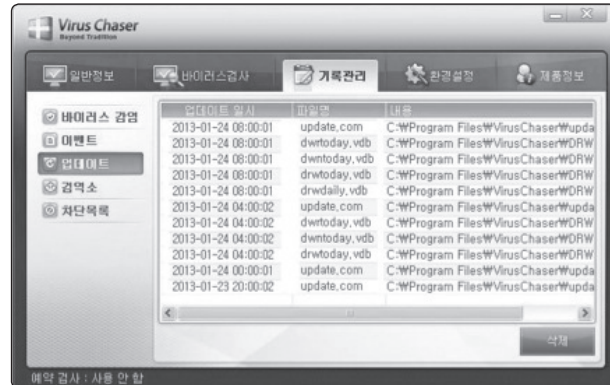
바이러스체이서 8.0에서 발생한 이벤트에 대한 기록을 열람 할 수 있습니다.
(업데이트 실시, 바이러스검사 기록, 서비스 시작/중지 등)



항 목	내 용
기록일시	이벤트가 발생한 일시
내 용	이벤트의 구체적인 내용

• 업데이트

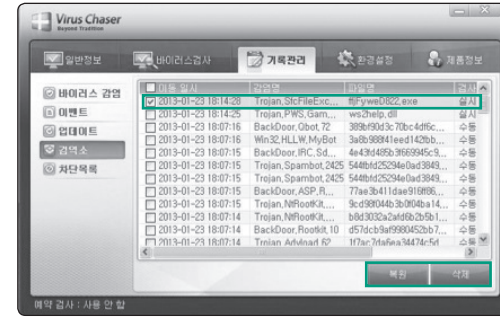
바이러스 패턴 업데이트에 대한 기록을 열람 할 수 있습니다.



항 목	내 용
업데이트일시	업데이트가 시행된 일시
파 일 명	업데이트 된 파일 명
내 용	업데이트 된 파일의 경로 및 파일명

• 검역소

바이러스로 진단된 원본 파일의 기록을 열람할 수 있으며, 기록된 행을 선택하여 복원 및 삭제가 가능합니다.



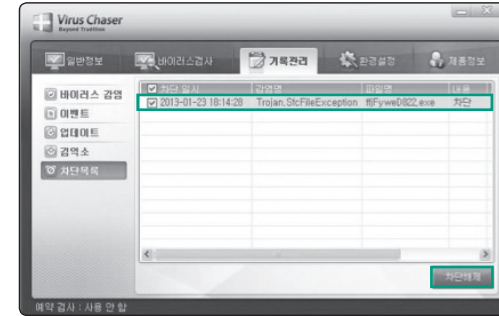
항 목	내 용
이동일시	바이러스로 검출 후 검역소로 이동된 일시
감 염 명	백업되어 있는 파일의 바이러스 명(진단명)
파 일 명	백업 되기 이전 원본 파일명
검사방법	바이러스로 검출 된 경위
파일경로	백업 되기 이전 원본 파일의 경로 및 파일명

복원을 원하는 파일을 선택 후 **복원** 버튼을 클릭하면 해당 파일이 백업 이전의 상태로 복원됩니다. 반대로, **삭제** 버튼을 클릭하면, 복원 불가능 한 상태로 영구 삭제 됩니다.

주의! 검역소 내에 백업되어 있는 파일들은 바이러스로 진단되어 치료되기 전 암호화 및 압축되어 저장된 파일로 복원 시 재 감염의 위험이 있으므로, 사용자의 각별한 주의가 필요합니다.

• 차단목록

실시간 감시에 의해 차단된 프로세스의 목록을 열람할 수 있습니다.
검역소에 저장 된 파일과는 별도로 실시간 감시에(프로액티브 엔진) 의해 차단된 프로세스 목록입니다.



항 목	내 용
차단일시	기록된 프로세스가 실시간 감시에 의해 차단 된 일시
감 염 명	차단될 당시 의심 행위에 따른 진단 명
파 일 명	차단된 프로세스의 이미지 파일명
내 용	차단 시 사용자의 조치 내용
파일경로	차단된 프로세스 이미지 파일의 경로 및 파일명

해제할 파일을 선택 후 **차단해제** 버튼을 누르면 해당 파일에 대해 차단이 해제됩니다.

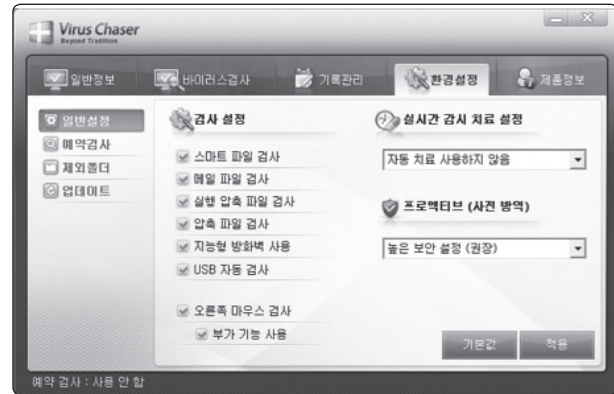
주의! 차단목록에 기록된 파일은 바이러스로 확정 또는 의심되어 차단된 파일이므로, 차단을 해제할 경우 바이러스의 활동이 재개 될 수 있으니 사용자의 각별한 주의가 필요합니다.

■ 환경설정

검사 설정, 업데이트 설정 등 바이러스체이서 8.0 기능에 대한 사용 환경을 설정할 수 있습니다.

• 일반설정

바이러스체이서 8.0의 기능 수행에 필요한 옵션을 설정 할 수 있습니다.
(바이러스 검사 설정, 실시간 감시 치료, 업데이트 방법, 예약 검사 일정, 제외 폴더를 설정할 수 있습니다.)

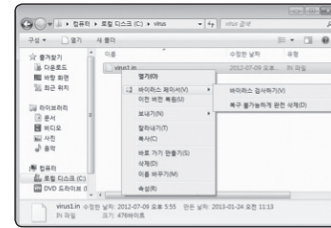


• 검사설정

항 목	내 용
스마트 파일 검사	스마트 파일 검사 여부 설정. 시스템 검사 이후 생성된 파일에 대한 검사와 운영 체제의 변경 사항에 대한 검사를 통해 더욱 빠른 검사 속도를 보장합니다.
메일 파일 검사	메일 파일 검사 여부 설정. 활성화 할 경우 dbx나 eml 파일과 같은 메일 파일에 대하여 검사를 진행합니다.
실행 압축 파일 검사	실행 압축 파일 검사 여부에 대한 설정. 체크할 경우 실행 압축 파일을 탐지 합니다.
압축 파일 검사	압축 파일 검사 여부에 대한 설정. 체크할 경우 압축 파일을 탐지 합니다.
지능형 방화벽 사용	TCP/IP 통신을 하는 프로그램이 악의적 행위를 할 경우 이를 차단 합니다. (실시간 감시)
USB 자동 검사	USB등 이동식 디스크 드라이브가 부착되면 자동으로 바이러스 검사를 실행합니다.

– 오른쪽 마우스 검사

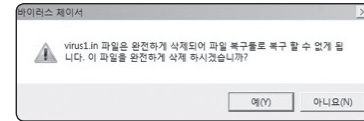
파일 및 폴더를 마우스 우측 버튼으로 클릭했을 때 바이러스 검사 메뉴의 표시 여부를 설정할 수 있습니다.



■ 주의

검사 설정에서 설정대상을 선택하지 않을 경우 기본적으로 바이러스만 검사되도록 설정되어 있습니다.

– 부가 기능 사용을 활성화하면 선택한 파일에 대해 복구가 불가능하도록 완전삭제(영구삭제) 할 수 있는 메뉴가 활성화 됩니다



“복구 불가능하게 완전 삭제”를 선택하면 위와 같이 확인 대화창이 나타나며, **예 (Y)** 를 눌렀을 경우 파일이 영구삭제 됩니다.

주의! “복구 불가능하게 완전 삭제” 옵션은 검역소 혹은 차단 목록에 백업을 하지 않기 때문에 삭제 시 사용자의 주의가 필요합니다.

• 실시간 치료 설정

항 목	내 용
사용자가 직접 치료	실시간 감시 중 바이러스가 탐지되면 팝업 창을 통해 사용자에게 알리고, 사용자의 조치를 유도합니다.
자동으로 치료	실시간 감시 중 바이러스가 탐지되면 자동으로 바이러스를 치료합니다.

• 프로액티브(사전 방역)

항 목	내 용
사용하지 않음	프로액티브 엔진에 의한 경고를 하지 않고, 시그니처 백신 엔진에 의해 등록된 바이러스만 진단합니다.
낮은 보안 설정	높은 보안 설정에서 제외되는 것을 포함해서 다음의 경우를 추가적으로 진단하지 않습니다. – 서비스에 프로그램 또는 ROOTKIT 드라이브를 등록하는 경우 – BHO에 DLL을 등록하는 경우 – 바탕 화면 아이콘을 생성하는 경우

항 목	내 용
높은 보안 설정	직접적인 바이러스의 감염 위험이 낮은 다음 경우를 제외한 모든 바이러스를 진단합니다. - 자신의 화면을 9초 동안 8번 이상 TOPMOST로 띄우는 것. - 사용자 동의 없이 바탕 화면에 바로가기 아이콘을 만드는 것. - Internet History 또는 Cookies 파일을 읽는 것. 사용자가 인지하는 상태에서는 허용되는 경우 - 다른 프로세스 메모리에 침투 하는 것. - 원격 프로세스 쓰레드를 생성 시키는 것. - 인터넷 익스플로러 설정을 바꾸는 것.
매우 높은 보안 설정	바이러스로 의심되는 모든 경우를 진단.

- 업데이트 설정 – 바이러스 체이서 8.0의 업데이트 형식을 변경할 수 있습니다.

항 목	내 용
수동 업데이트	자동 업데이트가 비활성화 되며, 모든 업데이트는 사용자의 수동 조작에 의해서만 이루어 집니다. 사용자가 실행하지 않는 경우 업데이트가 이루어지지 않으므로 보안상 취약하며 권장하지 않습니다.
자동 업데이트	설정한 시간(1시간, 2시간, 4시간[기본 값], 8시간)마다 업데이트가 백그라운드에서 자동으로 실행됩니다.

지정 시간 업데이트	사용자가 설정한 시간에만 업데이트가 백그라운드에서 자동으로 실행됩니다.
------------	---

- 예약 검사
사용자가 설정한 시간에 설정된 폴더들에 대한 바이러스 검사를 수행합니다.



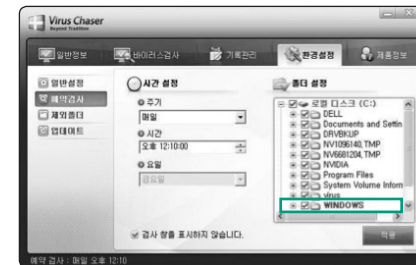
바이러스검사 주기에 대한 설정은 “사용 안 함”, “매일”, “매주”, “매월”을 선택 할 수 있습니다.

항 목	내 용
사용 안 함	예약검사를 사용하지 않습니다.
매 일	매일 지정된 시간에 바이러스 검사를 수행합니다. 매일을 선택할 경우 시간 설정 항목이 활성화 되고, 바이러스 검사를 수행할 시간을 설정할 수 있습니다.
매 주	매주 지정된 시간에 바이러스 검사를 수행합니다. 매주를 선택할 경우 시간과 요일 항목이 활성화 되고, 바이러스 검사를 수행할 시간과 요일을 설정할 수 있습니다.
매 월	매월 특정 날짜에 바이러스 검사를 수행합니다. 매월을 선택할 경우 시간과 날짜 항목이 활성화 되고, 바이러스 검사를 수행할 시간과 날짜를 설정할 수 있습니다.

- 제외 폴더
바이러스 검사에서 제외할 폴더를 추가할 수 있습니다. 제외할 폴더를 선택 후 적용을 누르면 해당 폴더 및 하위폴더는 모든 바이러스 검사(실시간 감시 및 수동/예약 검사)에서 제외됩니다.



제외폴더를 선택할 경우 예약 검사에서 제외된 폴더는 붉은색으로 표시가 되며, 해당 폴더의 상위 경로는 청록색으로 표시됩니다.



업데이트

업데이트를 설정할 수 있습니다. 제품번호, 서버주소, 업데이트 형식(수동/자동/지정시간 업데이트)을 사용자가 지정할 수 있습니다. 만약 프록시 서버를 사용하는 경우에는 프록시 설정을 체크하고 관련 정보를 입력하여야 합니다.



제품정보

바이러스체이서 8.0의 제품정보와 사용자 정보를 제공합니다.



제품 정보

바이러스체이서 8.0 프로그램의 버전, 제품번호, 적용기한을 표시합니다.

사용자 정보

바이러스체이서 8.0 프로그램의 설치정보로 사용자의 소속명칭, 사용자명, 서버스번호를 표시합니다.

[홈페이지](#) 바이러스체이서 홈페이지로 연결됩니다.

[사용설명](#) 사용설명서 페이지로 연결됩니다.

6.제거

[제어판] → [프로그램 추가/제거]에서 VirusChaser “변경/제거” 버튼을 클릭합니다. (Windows Xp 기준)



고객지원

바이러스체이서 8.0 제품을 구매한 고객이 제품을 사용하는 도중 발생하는 프로그램 문제 및 제품에 대한 문의를 하실 수 있습니다. 문의하시기 전, 사용설명서와 홈페이지 고객센터에 있는FAQ/고객상담실을 이용하여 문의사항에 대한 내용이 있는지 확인하시기 바랍니다. 문의사항에 대한 내용을 찾지 못한 경우 고객 지원 센터에 연락하시기 바랍니다.

고객 지원 센터 연락처

홈페이지 <http://www.viruschaser.com> **고객센터** <http://www.viruschaser.com> FAQ(자주묻는 질문)
<http://www.viruschaser.com> (1 : 1 상담)

이메일 영업문의 : sales@sgacorp.kr 기술문의 : cs@sgacorp.kr 바이러스문의 : cert@viruschaser.com

주소 137-896 서울특별시 서초구 마방로2길 44(양재동 315-1) SGA(주) 4층 고객지원센터 담당자 앞.

대표전화 070-7308-1004

트위터 @virus_chaser **페이스북** <http://www.facebook.com/viruschasercorp>