AhnLab

V3 Internet Security 9.0

AhnLab

일러두기

AhnLab V3 Internet Security 9.0 사용설명서의 내용과 프로그램은 저작권법에 의해서 보호받고 있습니다. 이 사용설명서에 표기된 제품명은 각 사의 등록상표입니다.

참고

본 프로그램에 포함된 7z 압축 해제 모듈은 http://www.7-zip.org 에 공개된 소스를 사용하였으며 LGPL을 따릅니다. LGPL은 설치 경로의 LGPL.TXT를 참고하시기 바랍니다. 수정한 7z의 소스는 http://www.ahnlab.com 에서 다운로드 할 수 있습니다.

표기 규칙

표기 규칙	표기 규칙 내용
< >	창의 이름입니다.(예: <설치 확인>)
>	메뉴 실행 순서입니다.(예: **시작>프로그램**)
굵은 글꼴	버튼 이름, 창에 나오는 메시지입니다.(예: **확인**)
참고	프로그램을 사용할 때 참고할 사항입니다.
주의	프로그램을 사용할 때 주의해야 할 사항입니다.

고객만족센터 연락처

- ❖ 홈페이지: http://www.ahnlab.com
- ❖ 주소: 463-400 경기도 성남시 분당구 삼평동 판교역로 220

목차

1장
제품 소개

1

제품 소개

AhnLab V3 Internet Security 9.0(이하 V3)은 다양한 보안 위협으로부터 기업의 클라어인트 PC를 안전하게 보호합니다. 특히 새로운 진단 기술 플랫폼인 다차원 분석 기반의 사전 방역 기술은 안전한 프로그램으로 검증되지 않은 프로그램을 사전 차단하여 안전한 PC 환경 구축에 기여합니다.

다차원 분석 플랫폼 기반의 탁월한 악성코드 탐지 및 진단율

새로운 V3는 안랩의 악성코드 통합 분석 및 대응 시스템인 다차원 분석 플랫폼을 기반으로 탁월한 진단율을 자랑합니다. 특히, 행위 기반 기술 및 평판 기반 기술로 검증되지 않은 프로그램의 실행을 사전에 차단하는 사전 방역 기능을 제공해 안심하고 PC를 사용하실 수 있습니다.

독자 개발한 엔진 및 스마트 검사 기술의 차별적인 검사 속도

최초 1회 검사로 안전성 확보 후 새로운 파일 및 변환된 파일을 검사하는 스마트 검사(Smart Scan) 기술로 6배 이상 빨라진 검사 속도를 체감할 수 있습니다. 또한, 20년 이상 축적된 안랩의 악성코드 분석 기술로 독자 개발한 TS엔진, ASD 엔진 등을 적용해 더욱 신속하고 정확하게 악성코드를 검사합니다.

초경량 엔진으로 시스템 부담 최소화

독자적인 엔진 최적화 기술과 6억개 이상의 ASD(AhnLab Smart Defense) 데이터베이스, DNA 규칙 적용으로 PC의 메모리 사용을 최소화하여 PC 메모리 사용량은 줄이고 사용자 편의성과 진단율을 극대화했습니다.

클라우드 기반의 악성코드 분석 및 대응 기술로 신/변종 위협 대응

클라우드 기반의 ASD(AhnLab Smart Defense) 기술 및 ASD 네트워크를 통한 위협 정보 공유로 다양한 신종 위협에 더욱 신속하고 정확하게 대응할 수 있습니다.

쉬운 컬러, 메인 화면에서 문제 한 번에 해결

선명하고 이해하기 쉬운 컬러로 PC의 보안 상태를 표시하여 사용자가 보안 상태를 쉽게 인지하여 문제를 해결할 수 있습니다. 또한, V3의 주요 검사 기능과 엔진 업데이트, ASD 클라우드 서버 현황을 HOME 화면에서 바로 확인할 수 있어 이용이 간단합니다.

주요 기능

V3는 악성코드 진단과 치료를 위해 기존의 악성코드 진단/치료 방법과 클라우드 자동 분석 기술을 도입하여 사용자 PC에서 실행되는 의심 파일을 실시간으로 분석하고 치료 정보를 제공하여 사용자 스스로 PC를 보다 빠르고 안전하게 지킬 수 있습니다.

다양한 PC 검사 기능을 통한 바이러스, 웜 등 악성코드 진단 및 치료

PC 실시간 검사, 빠른 검사, 정밀 검사, 탐색기 검사 등의 다양한 PC 검사 기능을 통해 바이러스, 스파이웨어, 웜, 트로이목마 등 악성코드를 정확하게 진단하고 치료합니다.

ASD 클라우드 진단을 통한 신종/변종 악성코드 검사

안랩 클라우드 서버에 정보가 없는 새로운 파일을 발견했을 경우 클라우드 자동 분석과 진단을 통해 새로운 파일의 악성코드 감염 여부를 실시간 분석하고 분석 정보를 사용자에게 제공합니다. 클라우드 자동 분석 기능을 활용하면 클라우드 사용자의 평판 정보와 실시간 분석을 통해 악성코드에 빠르게 대처할 수 있습니다.

의심스러운 웹사이트 접속 차단을 통한 웹 보안 강화

안랩 클라우드 서버의 웹사이트 정보를 바탕으로 사용자가 접속하는 사이트에 대한 다양한 분석 정보를 제공합니다. 사용자가 유해 사이트, 피싱 사이트, 불필요한 사이트로 알려진 웹사이트에 접속한 경우 접속을 차단합니다. 웹 보안 기능을 활용하면 사용자 모르게 악성코드를 배포하거나 실행하는 웹사이트의 접속을 차단하여 사용자 PC를 안전하게 지키는데 도움이 됩니다.

의심 프로그램 실행 차단과 삭제를 통한 강력한 보안 기능

안랩 클라우드 서버의 평판 기반 진단 기능을 통해 사용자 PC에서 의심스러운 파일이 실행될 경우 평판 정보를 바탕으로 파일의 실행을 차단합니다. 클라우드 평판 기반 진단은 안랩 클라우드 서버에 연결된 사용자들이 신뢰하거나 차단한 파일에 대한 정보, 사용자들이 신고한 파일에 대한 의심 행위를 기반으로 파일을 진단합니다.

PC 관리와 백업을 위한 다양한 기능 및 분석 정보 제공

PC 최적화, PC 복구와 같은 PC 사용의 효율성과 백업을 담당하는 기능을 통해 사용자 PC를 보다 빠르고 안전하게 이용할 수 있게 도와줍니다. 또한, 파일 분석 보고서와 사이트 분석 보고서, 클라우드 자동 분석 보고서를 통해 사용자 PC에서 발견한 의심 파일과 의심 행위에 대한 정보를 자세하게 확인할 수 있어 능동적으로 PC의 보안 점검을 수행할 수 있습니다.

2장
설치하기

시스템 사양

V3를 설치하기 위해서는 다음의 시스템 사양 이상의 하드웨어 사양과 소프트웨어 환경을 만족해야 합니다. 시스템 사양을 확인하신 후에 설치하여 주시기 바랍니다.

⚠ 주의

다음의 시스템 사양 이상의 하드웨어와 소프트웨어 환경을 만족하지 않는 경우 프로그램이 정상 작동하지 않을 수 있으며, 안랩은 이로 인한 책임을 지지 않습니다.

하드웨어 최소 사양

- CPU: Intel Pentium4 1GHz 이상(Windows XP의 경우 300MHz 이상)
- 메모리: 512MB 이상
- HDD: 300MB 이상의 여유 공간
- NIC: 10/100 Ethernet Card
- 해상도: 800x600 256 컬러 이상

웹브라우저

- Microsoft Internet Explorer 6.0 이상

지원 언어

- 한국어
- 영어

소프트웨어 최소 사양

- Microsoft Windows XP SP2
- Microsoft Windows VISTA
- Microsoft Windows 7
- Microsoft Windows 8

참고

지원 가능한 운영 체제는 32비트와 64비트를 모두 지원합니다.

설치하기

V3 설치 파일을 실행하면, PC에 V3를 설치할 수 있습니다.

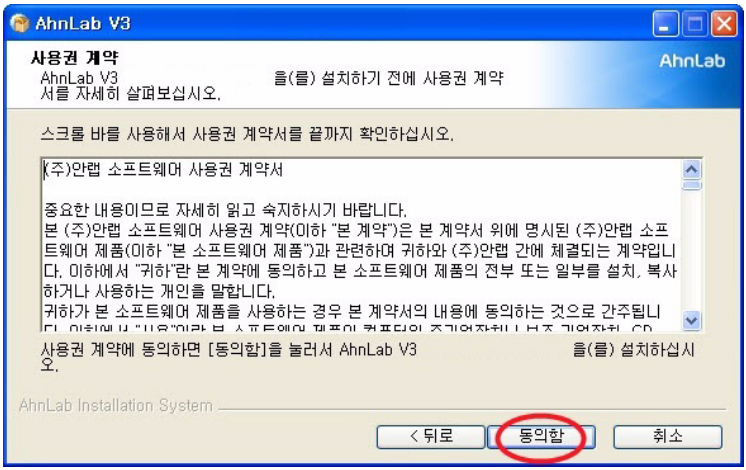
참고

V3를 설치하기 전에 이전에 설치한 V3 프로그램이나 타사 백신 프로그램을 미리 제거하여 주시기 바랍니다.

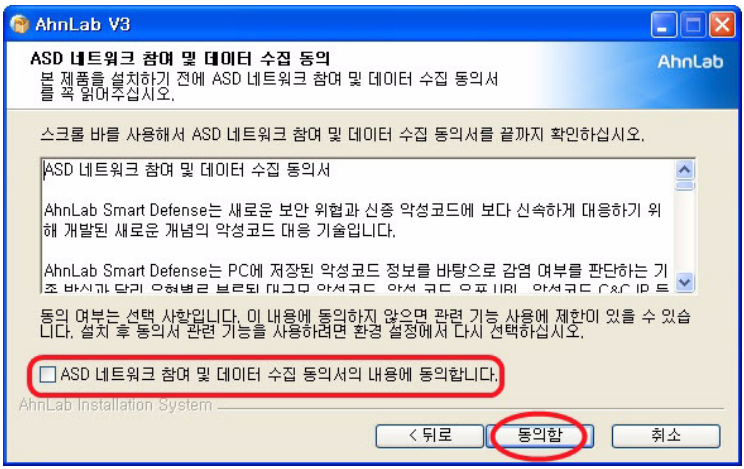
1 V3 설치 파일을 실행합니다.

2 설치 시작 화면이 나타나면 **다음**을 누릅니다.

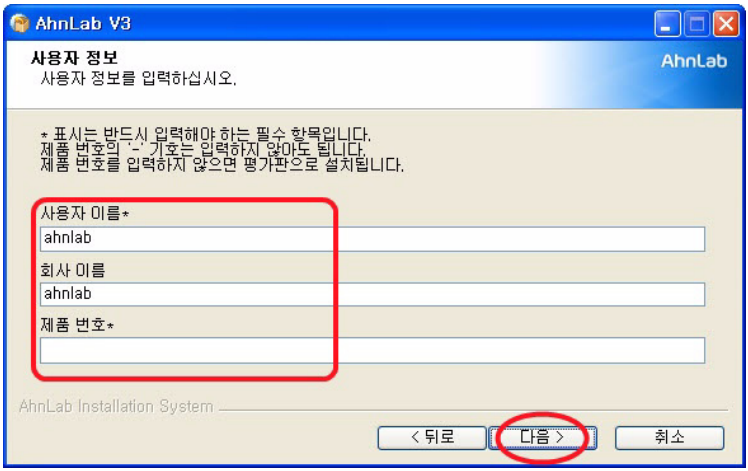
3 <사용권 계약>이 나타나면, (주)안랩 소프트웨어 사용권 계약서의 내용을 잘 읽어주시기 바랍니다. 사용권 계약의 내용에 동의하면 **동의함**을 누릅니다.



4 <ASD 네트워크 참여 및 데이터 수집 동의>가 나타나면 ASD 네트워크 참여 및 데이터 수집 동의서의 내용을 잘 읽어주시기 바랍니다. **ASD 네트워크 참여 및 데이터 수집 동의서의 내용에 동의합니다.**를 선택하면 설치를 계속할 수 있습니다. **동의함**을 누릅니다.



5 <사용자 정보>가 나타나면 **사용자 이름, 회사 이름, 제품 번호**를 입력합니다.

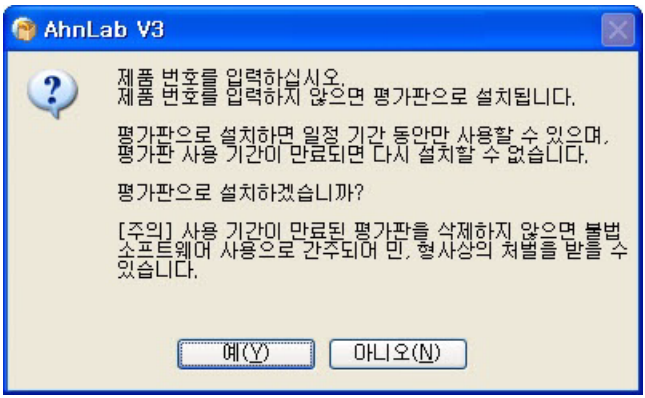


참고

* 표시가 되어 있는 사용자 이름과 제품 번호는 반드시 입력해야 합니다. 제품 번호의 경우 설치 후 V3 HOME 화면에서 제품 번호를 등록할 수 있습니다. 제품 번호를 입력하지 않으면, 평가판으로 설치됩니다.

참고

설치 과정에서 제품 번호를 입력하지 않으면 다음과 같은 메시지 창이 표시됩니다.



6 <설치 폴더> 선택 화면이 나타나면 V3를 설치할 폴더를 선택합니다. **찾아보기...**를 누르면, 기본 설치 폴더 이외의 폴더를 직접 선택할 수 있습니다. **설치**를 누릅니다.

7 <설치 진행> 화면이 나타나면서 PC에 설치 파일을 복사하는 과정이 나타납니다. 설치가 끝날때까지 잠시 기다려 주시기 바랍니다.

8 설치를 마치면, 설치 마침 화면이 나타납니다. **마침**을 누르면 설치 화면이 사라집니다.

제품 번호 등록

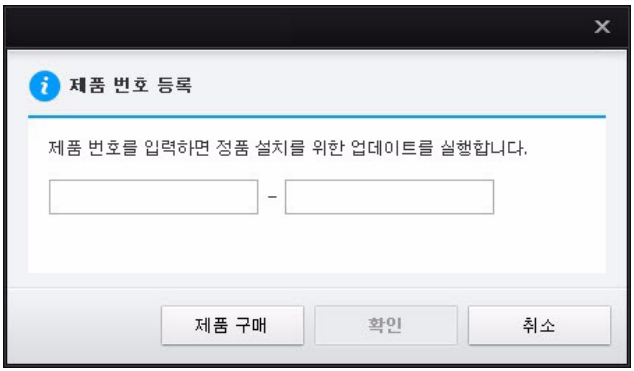
V3 정품을 구입한 사용자는 제품 번호를 등록해야 합니다. 제품 번호를 등록하지 않으면 엔진을 업데이트할 수 없으므로 최신 악성코드로 인한 피해를 예방하거나 진단/치료할 수 없습니다. 제품 번호 등록은 설치 과정에서 등록할 수 있습니다. 설치 과정에서 제품 번호를 등록하지 않은 경우에는 제품 설치 후 HOME 화면에서 제품 번호 등록을 해 주시기 바랍니다.

HOME 화면에서 제품 번호 등록

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 HOME 화면의 보안 상태 표시 영역에서 **제품 번호 등록**을 누릅니다.

3 <제품 번호 등록>이 나타나면, 제품 구입시 발행된 제품 번호를 입력해 주십시오.



참고

제품 구매를 누르면 안랩닷컴에서 제품을 구입하실 수 있습니다.

4 제품 번호를 입력한 후 **확인**을 누릅니다.

5 **제품 번호를 등록했습니다.** 라는 메시지가 나타나면 **확인**을 누르십시오.

6 업데이트 필요 여부를 확인한 후 **제품 인증을 마쳤습니다.** 라는 메시지가 나타나면 정품 등록이 완료된 것입니다.

온라인 등록

2

제품 번호 등록을 마친 사용자는 안랩닷컴에서 온라인 등록을 해 주시기 바랍니다. 온라인 등록을 하면, 정품 사용자에게 제공하는 다양한 서비스를 이용하실 수 있습니다.

HOME 화면에서 온라인 등록

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 HOME 화면의 보안 상태 표시 영역에서 **온라인 등록**을 누릅니다.

3 안랩닷컴의 온라인 등록 페이지로 이동합니다. 등록 페이지의 내용에 따라 온라인 등록을 해 주십시오.

참고

온라인 등록을 하려면 안랩닷컴에 회원 가입이 되어 있어야 하며 온라인 등록을 위해서는 로그인을 해야 합니다.

제거하기

V3를 PC에서 제거하기 위한 방법은 다음과 같습니다.

⚠ 주의

V3를 제거하기 전에 실행 중인 프로그램과 데이터는 미리 저장하시고, Internet Explorer는 실행을 종료하십시오.

제어판에서 제거하기

1 **시작>제어판**을 실행합니다.

2 **프로그램 및 기능**을 선택합니다.

3 프로그램 제거 또는 변경 목록의 **AhnLab V3 Internet Security 9.0**에서 마우스 오른쪽을 누르고 **제거**를 선택합니다.

참고

Windows XP의 경우에는 **시작>제어판>프로그램 추가/삭제**의 현재 설치된 프로그램 목록에서 AhnLab V3 Internet Security 9.0을 선택하고 **제거**를 누르면 프로그램을 삭제할 수 있습니다.

시작 메뉴에서 제거하기

❖ **시작>모든 프로그램>AhnLab>AhnLab V3 Internet Security 9.0>AhnLab V3 Internet Security 9.0 제거**를 선택합니다.

제거 진행 과정

1 <프로그램 제거>가 나타나면 **제거**를 누릅니다.

2 <제거 진행>에서 프로그램에 관련된 서비스와 파일을 삭제하는 과정이 나타납니다. 제거가 끝날때까지 잠시 기다려 주십시오.

참고

제거 진행 중에 **일부 파일은 탐색기(Explorer.exe)를 재시작해야 삭제가 됩니다. 지금 탐색기를 재시작 하시겠습니까?** 라는 메시지가 나타날 수 있습니다. 제거를 위해 **예**를 선택할 것을 권장합니다.

3 파일 삭제 과정을 마친 후, **프로그램 제거를 끝내려면 컴퓨터를 다시 시작해야 합니다. 지금 다시 시작하겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 컴퓨터를 다시 시작하고, **아니오**를 누르면 컴퓨터를 다시 시작하지 않습니다. 안전한 삭제를 위해 예를 선택하여 컴퓨터를 다시 시작할 것을 권장합니다.

3장
둘러보기

실행 방법

V3를 실행하는 방법입니다.

3

바탕 화면에서 실행하기

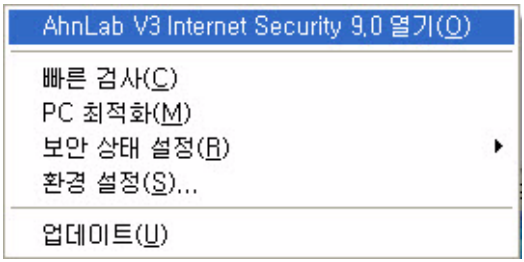
❖ 바탕 화면의 V3 바로가기 아이콘( )을 더블 클릭합니다.

시작 메뉴에서 실행하기

❖ **시작>모든 프로그램>AhnLab>AhnLab V3 Internet Security 9.0>AhnLab V3 Internet Security 9.0**을 선택합니다.

작업 표시줄에서 실행하기

❖ 작업 표시줄의 V3 아이콘( )에서 마우스 오른쪽을 누르고 **AhnLab V3 Internet Security 9.0 열기**를 선택합니다.



업데이트하기

V3 설치를 마쳤으면 가장 먼저 최신 엔진으로 업데이트할 것을 권장합니다. 백신 프로그램은 최신 엔진의 업데이트를 적용한 후에 악성코드를 검사해야 새로 발견된 악성코드까지 검사/치료할 수 있습니다.

HOME 화면에서 실행하기

❖ V3 실행 후 HOME 화면에서 업데이트를 실행할 수 있습니다.

작업 표시줄에서 실행하기

❖ 작업 표시줄의 V3 아이콘( )에서 마우스 오른쪽을 누르고 **업데이트**를 선택합니다.

업데이트 진행 메시지

작업 표시줄에서 업데이트를 실행하면 업데이트 진행 단계별로 다음과 같은 메시지가 화면에 나타납니다.

❖ 업데이트를 준비하고 있습니다.: 업데이트를 실행한 후 처음 나타나는 메시지로 업데이트를 위한 준비 과정입니다.

❖ 업데이트할 파일을 검색하고 있습니다.: 업데이트 대상 파일을 검색하는 단계입니다.

❖ 업데이트를 마쳤습니다.: 업데이트 파일을 다운로드하여 적용을 마친 경우입니다.

❖ 업데이트를 실패했습니다.(오류 코드: ****): 업데이트를 실패한 경우입니다. 오류 코드에 업데이트를 실패한 이유에 대한 코드 번호를 출력합니다. 재시도해도 동일한 문제가 계속되면 고객만족센터로 오류 코드를 알려주십시오.

- ❖ 업데이트를 위해 시스템을 분석하고 있습니다.: 업데이트 적용을 위해 PC를 분석하고 있는 경우입니다.
- ❖ 업데이트 파일을 복사하고 있습니다.: 업데이트 파일을 다운로드한 후 PC에 복사하는 과정입니다.
- ❖ 업데이트를 위해 중지했던 프로세스를 다시 시작합니다.: 업데이트를 하기 위해 중지했던 V3 프로세스를 다시 시작하는 과정입니다.
- ❖ 제품 인증을 요청하고 있습니다.: 정품 인증을 위해 제품 번호를 확인하는 과정입니다.
- ❖ 제품 인증을 마쳤습니다.: 정품 인증을 완료한 경우입니다.
- ❖ 제품 인증을 실패했습니다.(오류 코드: ****): 설치된 제품의 제품 번호로 제품 인증을 하지 못한 경우입니다. 제품 번호를 다시 한번 확인해 주십시오. 제품 번호에 문제가 없다면 사용 기간이 만료되었을 수도 있습니다. 제품 번호와 사용 기간에 문제가 없다면 고객만족센터로 문의해주십시오.
- ❖ 등록되지 않은 제품번호입니다.: 제품 설치 후 제품 번호 등록을 하지 않은 경우입니다. 제품 번호를 등록하여 정품으로 등록하여 주십시오.
- ❖ 업데이트 파일을 다운로드하고 있습니다.: 업데이트 서버에서 파일을 다운로드하고 있는 단계입니다.
- ❖ 이 메시지는 **초 후에 자동으로 사라집니다.: 업데이트 진행 메시지 창이 몇 초 후에 자동으로 사라지는 것을 알려줍니다.

참고

업데이트에 대한 자세한 내용은 업데이트를 참고하십시오.

검사하기

최신 엔진으로 업데이트한 후에는 바로 PC 전체를 검사하여 백신 프로그램 설치 이전에 감염된 파일이 있는지 확인하는 것이 좋습니다. 백신 설치 후 처음 실행하는 검사는 정밀 검사를 권장합니다. 정밀 검사는 검사 영역과 대상을 사용자가 직접 선택하여 검사할 수 있으며 백신 설치 이전에 감염된 파일까지 검사할 수 있으므로 처음 검사는 정밀 검사를 실행하시기 바랍니다.

정밀 검사 실행 방법

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3 HOME 화면에서 **고급 화면**을 선택합니다.

3 **정밀 검사** 탭을 누릅니다.

4 검사 영역을 선택합니다.

5 **검사 시작**을 누릅니다.

참고

정밀 검사에 대한 자세한 내용은 정밀 검사를 참고하십시오.

다양한 PC 검사 기능

V3에서는 정밀 검사 이외에도 다양한 검사 기능을 제공합니다. 사용자의 PC 환경이나 작업 환경에 맞는 검사를 선택하여 주기적으로 검사할 것을 권장합니다.

- ❖ PC 실시간 검사: 메모리에 상주하여 파일의 복사, 이동, 실행과 같은 행위를 검사합니다. 감염된 파일이 발견된 경우 사용자에게 감염 여부를 알려주고 자동 치료하거나 설정된 치료 방법에 따라 처리합니다.
- ❖ 빠른 검사: 감염 위험이 높은 중요 폴더와 파일을 검사합니다.
- ❖ 정밀 검사: 사용자가 직접 검사 영역과 검사 대상을 선택하여 검사합니다.
- ❖ 예약 검사: 사용자가 선택한 날짜와 시간에 PC를 검사합니다.
- ❖ 탐색기 검사: Internet Explorer의 탐색기나 바탕 화면에서 폴더나 파일을 선택하여 검사합니다.
- ❖ USB 드라이브 검사: USB 드라이브를 인식하는 순간 해당 드라이브의 감염 여부를 검사합니다.

작업 표시줄

3

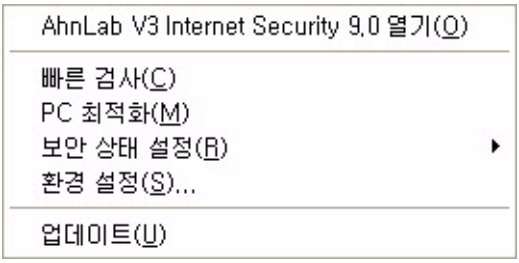
V3를 설치하면 작업 표시줄에 알림 아이콘( )이 등록됩니다. V3는 작업 표시줄의 알림 아이콘 색상이나 모양에 따라 현재 V3의 상태를 표시합니다. 작업 표시줄의 알림 아이콘에서 마우스 오른쪽을 누르면 V3의 주요 기능을 간단히 실행할 수 있습니다.

작업 표시줄의 알림 아이콘

- ❖ : V3의 PC 실시간 검사가 작동하고 있는 경우입니다.
- ❖ : V3의 PC 실시간 검사가 꺼져 있는 경우입니다.
- ❖ : 예약 검사에서 설정한 주기에 예약 검사를 실행하고 있는 경우입니다.
- ❖ : PC 실시간 검사가 꺼진 상태에서 예약 검사를 실행하고 있는 경우입니다.

작업 표시줄에서 실행할 수 있는 기능

작업 표시줄의 V3 아이콘( )에서 마우스 오른쪽을 누르면 V3의 주요 기능을 실행할 수 있습니다.



- ❖ AhnLab V3 Internet Security 9.0 열기: AhnLab V3 Internet Security 9.0 프로그램의 HOME 화면을 보여줍니다.
- ❖ 빠른 검사: 악성코드의 감염 위험이 높은 중요 폴더와 파일을 검사하는 빠른 검사를 실행합니다. 빠른 검사를 실행하면, 빠른 검사 진행 화면이 나타납니다.
- ❖ PC 최적화: 필요없는 파일과 레지스트리 정보, 임시 파일을 청소하고 메모리 사용을 최적화하는 PC 최적화를 실행합니다.

❖ 보안 상태 설정: PC 보호를 위해 실시간 작동하는 PC 실시간 검사, 웹 보안, 개인 방화벽, 네트워크 침입 차단, 행위 기반 침입 차단을 실행하거나 실행을 중지할 수 있습니다.

❖ 환경 설정: V3에서 제공하는 기능에 대한 옵션을 설정할 수 있습니다. PC 검사, 웹 보안, Active Defense 등 각 기능별로 사용자 환경에 맞게 설정할 수 있습니다.

❖ 업데이트: 업데이트를 즉시 실행합니다.


AhnLab

4장
HOME

화면 구성

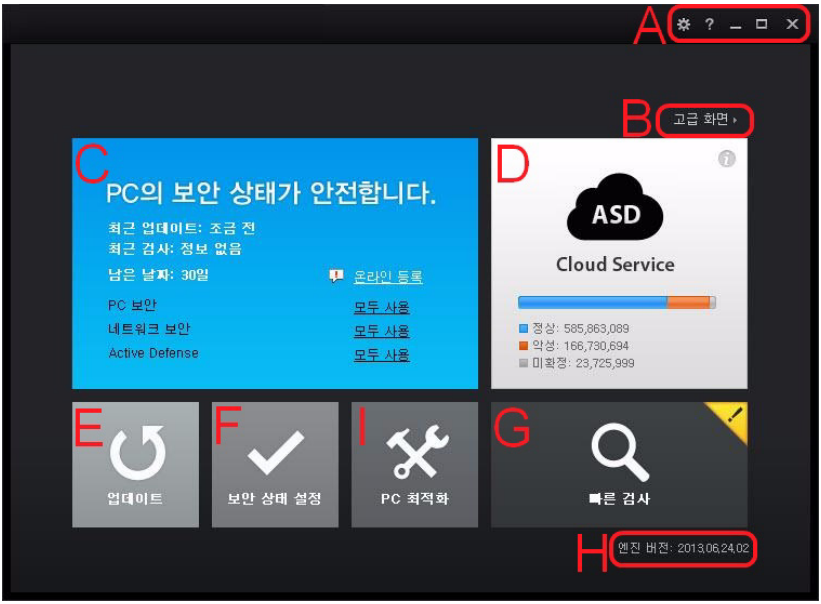
V3를 실행하면 가장 먼저 나타나는 HOME 화면에서는 V3의 보안 상태와 클라우드 현황 등의 현황 정보를 확인할 수 있습니다. 또한, V3에서 사용할 수 있는 검사와 업데이트, PC 관리를 위한 최적화를 실행할 수 있습니다.

4

참고

V3의 시작 화면은 환경 설정에서 설정한 내용에 따라 HOME 화면이 표시되거나 고급 화면이 표시될 수 있습니다. 환경 설정>기타 설정>사용 환경>사용자 설정에서 시작 화면을 고급 화면으로 선택한 경우에는 HOME 화면이 고급 화면으로 표시됩니다. 시작 화면을 고급 화면으로 설정한 경우에는 보안 센터의 내용을 참고하십시오. 본 설명에서는 시작 화면이 HOME 화면으로 설정된 경우에 대해 설명합니다.

HOME 화면



A 영역

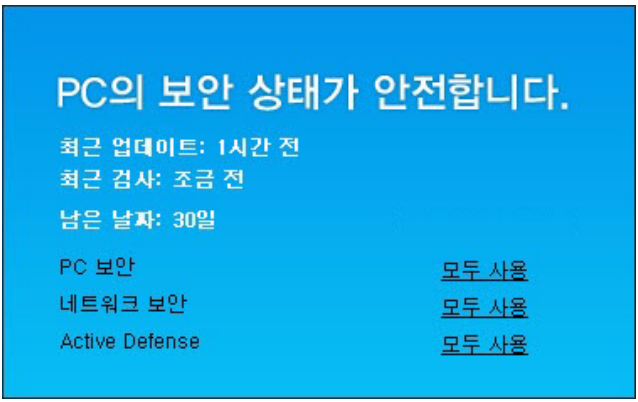
- ❖ : 환경 설정을 실행합니다. 환경 설정에서는 V3 사용에 관련된 각종 옵션을 설정할 수 있습니다.
- ❖ : V3의 도움말을 실행합니다. V3 도움말은 인터넷을 통해 웹페이지에서 확인할 수 있습니다.
- ❖ : 화면을 최소화합니다.
- ❖ : 화면을 최대화합니다. 화면을 최대화한 상태에서 를 누르면 원래 사이즈로 돌아옵니다.
- ❖ : 현재 화면을 닫습니다.

B 영역

고급 화면으로 화면을 전환합니다. 고급 화면에서는 보안 센터, 정밀 검사, 네트워크 보안, Active Defense, 도구 탭을 선택할 수 있습니다.

C 영역

제품 사용 정보와 PC 보안, 네트워크 보안, Active Defense 사용 여부에 따른 보안 상태를 색깔별로 표시합니다. PC 보안, 네트워크 보안, Active Defense 옆에 표시된 **사용 안 함**이나 **모두 사용**, **일부 사용**을 선택하면 <보안 상태 설정>에서 해당 기능의 사용 여부를 다시 선택할 수 있습니다.



- ❖ 최근 업데이트: 최근 업데이트 실행 시기를 표시합니다.
- ❖ 최근 검사: 최근에 검사를 실행한 시기를 표시합니다.

❖ 남은 날짜: 제품 번호를 등록하지 않고 평가판을 설치하여 사용하는 경우 평가판 사용 만료까지 남은 기간을 표시합니다.

❖ 제품 번호 등록: 제품 번호를 등록하지 않고 평가판을 설치하여 사용하는 경우에 표시됩니다. 제품 번호 등록을 누르면, <제품 번호 등록>에서 정품 설치를 위한 제품 번호를 입력하거나 제품 구매를 선택할 수 있습니다.

❖ 온라인 등록: 제품 번호 등록 후 고객 등록을 하지 않은 경우입니다. 온라인 등록을 누르면, 안랩닷컴의 온라인 제품 등록 페이지로 이동합니다.

❖ 파란색: PC 보안, 네트워크 보안, Active Defense 관련 기능을 모두 사용하고 있는 경우로 안전함을 의미합니다.

❖ 노란색: PC 보안, 네트워크 보안, Active Defense 관련 기능 중 일부를 사용하지 않는 경우로 주의를 의미합니다.

❖ 주황색: PC 실시간 검사를 사용하지 않는 경우로 위험을 의미합니다.

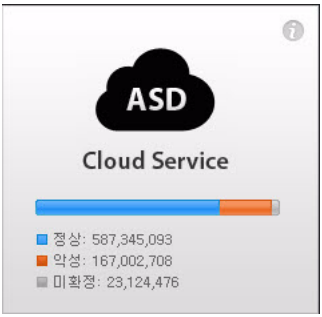
❖ 해결하기: 보안 상태가 주의나 위험인 경우에 **해결하기**를 누르면 PC를 점검하여 보안 상태를 안전하게 설정합니다.

참고

해결하기 진행 중에 문제가 발생할 경우에는 안랩닷컴 > 고객지원> 온라인고객지원 > FAQ의 검색어 입력란에 **해결하기**를 입력하여 해결 방법을 참고하시기 바랍니다.

D 영역

안랩 클라우드 서버의 현황 정보를 표시합니다.



❖ 정상: 클라우드 서버에 보고된 파일 중 악성코드가 아닌 정상 파일로 분류된 파일의 개수를 표시합니다.

❖ 악성: 클라우드 서버에 보고된 파일 중 악성코드로 분류된 파일의 개수를 표시합니다.

❖ 미확정: 클라우드 서버에 보고되었지만 정상과 악성 여부가 결정되지 않은 파일의 개수를 표시합니다.

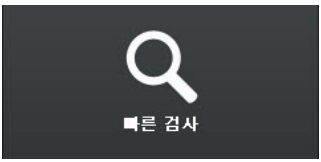
E 영역

업데이트를 실행합니다. 업데이트를 누르면, 안랩 업데이트 서버에 접속하여 최신 엔진 파일로 업데이트합니다.

F 영역

보안 상태를 설정합니다. 보안 상태를 선택하면, <보안 상태 설정>에서 PC 보안, 네트워크 보안, Active Defense에 관련된 보안 기능을 ON하거나 OFF할 수 있습니다.

G 영역



빠른 검사를 실행합니다. 빠른 검사는 프로세스 영역, 부트 영역, 중요 시스템 영역과 같은 중요 폴더를 검사하는 기능입니다.

H 영역

현재 사용 중인 엔진 버전을 표시합니다.

I 영역

PC 최적화를 실행합니다. PC 최적화는 필요없는 임시 파일과 메모리를 정리하여 PC 사용과 인터넷 연결 개선에 도움이 됩니다.

보안 상태 설정

보안 상태 설정은 V3가 PC를 실시간으로 보호하는 기능을 한 화면에 모아놓은 기능입니다. 보안 상태 설정에서는 각 보안 기능의 실행 여부를 한 눈에 확인할 수 있으며, 각 보안 기능의 사용 여부를 선택할 수 있습니다. 보안 상태에서 설정한 기능의 실행 여부에 따라 V3 HOME 화면의 색상이 변경됩니다. 모든 보안 기능을 실행하여 안전한 경우는 파란색, 일부 기능을 사용하지 않아 보안 상태에 주의를 필요로 하는 경우에는 노란색, PC 실시간 검사를 실행하지 않은 경우에는 위험을 표시하는 주황색으로 상태 정보를 제공합니다.

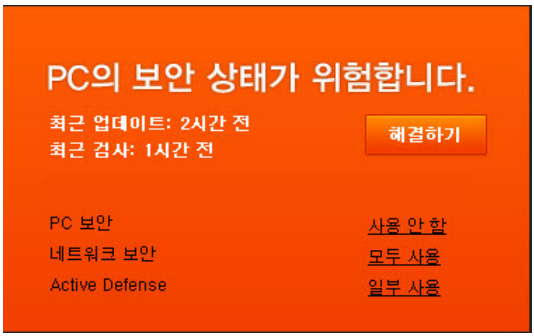
보안 상태 설정 실행

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

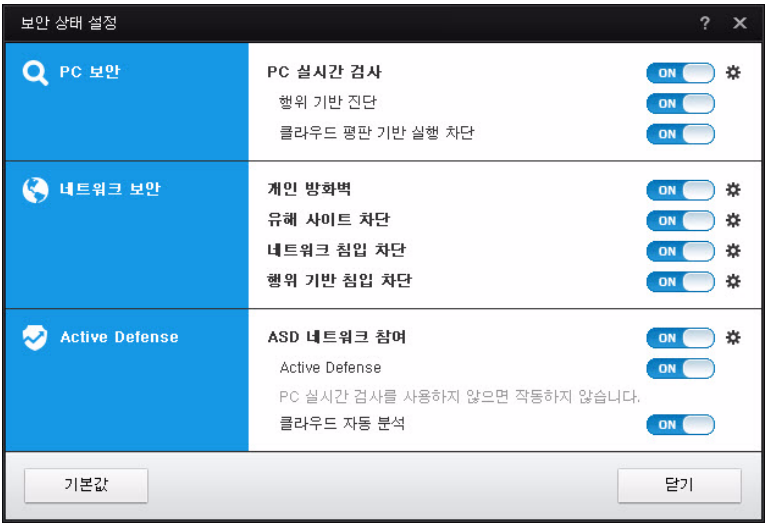
2 V3가 실행되면 HOME 화면의 **보안 상태 설정**을 누릅니다.

참고

보안 상태 표시 영역에서 **사용 안 함/모두 사용/일부 사용**을 눌러 <보안 상태 설정>을 실행할 수도 있습니다.



3 <보안 상태 설정>이 나타납니다.



참고

각 항목의 ON/OFF 옆에 있는 ⚙아이콘을 누르면 각 해당 기능의 환경 설정으로 이동합니다.

참고

작업 표시줄의 V3 아이콘에서 마우스 오른쪽을 눌러 보안 상태 설정을 선택하면, 작업 표시줄에서도 보안 상태 관련 기능을 ON/OFF할 수 있습니다.

PC 보안

PC 보안에 관련된 기능의 사용 여부를 선택할 수 있습니다. 사용 여부를 선택할 수 있는 기능은 다음과 같습니다.

- ❖ PC 실시간 검사: 사용자 PC에서 발생하는 파일의 저장, 이동, 실행, 삭제, 네트워크 접근 등의 일련의 행위를 탐지하여 감염된 악성코드가 있는 경우 치료 방법에 따라 처리합니다.
- ❖ 행위 기반 진단: 다양하고 입체적인 방법으로 악성코드를 사전 대응하는 기술로 파일이 실행될 때 작동하는 행위에 대한 일련의 의심 행위 세트를 기반으로 악성코드를 진단합니다.
- ❖ 클라우드 평판 기반 실행 차단: 안랩 클라우드 서버의 평판 정보를 기반으로 하여 평판 점수가 낮은 프로그램의 실행을 차단합니다.

참고

PC 실시간 검사를 ON으로 설정하지 않은 경우에는 행위 기반 진단과 클라우드 평판 기반 실행 차단도 사용 여부를 설정할 수 없으며, 해당 기능이 작동하지 않습니다.

네트워크 보안

네트워크 보안에 관련된 기능의 사용 여부를 선택할 수 있습니다. 사용 여부를 선택할 수 있는 기능은 다음과 같습니다.

- ❖ 개인 방화벽: 네트워크 규칙과 프로그램 규칙에 따라 허가하지 않은 인터넷 연결을 차단하여 PC를 안전하게 유지할 수 있습니다.
- ❖ 유해 사이트 차단: 홈페이지 변조를 통해사용자들이 해당 사이트에 접속했을 때 악성코드를 다운로드하게 하는 유해 사이트 접속을 차단합니다.
- ❖ 네트워크 침입 차단: 패킷의 특정 서명 정보를 기반으로 악성코드를 탐지합니다.
- ❖ 행위 기반 침입 차단: 비정상적인 패킷의 흐름을 모니터링하여 이상 여부를 탐지합니다.

Active Defense

Active Defense에 관련된 기능의 사용 여부를 선택할 수 있습니다. 사용 여부를 선택할 수 있는 기능은 다음과 같습니다.

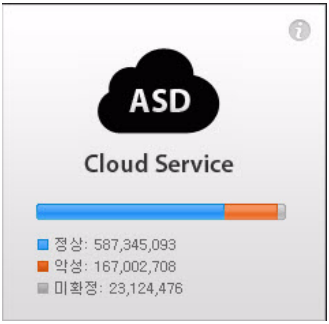
- ❖ ASD 네트워크 참여: ASD 네트워크 사용에 동의합니다.
- ❖ Active Defense: PC에서 실행되는 프로그램이 의심 행위를 하는지를 판단하고 점검합니다.
- ❖ 클라우드 자동 분석: ASD 클라우드 서버에 보고되지 않은 파일을 클라우드 자동 분석 서버로 전송하여 분석 결과를 제공합니다.

참고

PC 실시간 검사를 사용하지 않으면 Active Defense는 작동하지 않습니다.

ASD 클라우드 현황 정보

안랩 클라우드 서버는 안랩 클라우드 서버에 연결된 사용자들이 전송한 파일과 알려진 파일에 대한 분석 정보를 보관하고 있습니다. ASD 클라우드 현황 정보에서는 클라우드 서버의 데이터베이스를 바탕으로 악성코드에 감염되지 않은 정상 파일의 개수, 악성 파일의 개수, 미확정 파일에 대한 현황 정보를 표시합니다.



❖ 정상: 클라우드 서버에 보고된 파일 중 악성코드가 아닌 정상 파일로 분류된 파일의 개수를 표시합니다.

❖ 악성: 클라우드 서버에 보고된 파일 중 악성코드로 분류된 파일의 개수를 표시합니다.

❖ 미확정: 클라우드 서버에 보고되었지만 정상과 악성 여부가 결정되지 않은 파일의 개수를 표시합니다.

참고

인터넷 연결에 문제가 있어 안랩 클라우드 서버에 접속하지 못했을 경우에는 **네트워크 문제로 클라우드 정보를 가져올 수 없습니다.** 라는 메시지가 해당 영역에 표시됩니다. 인터넷 연결을 확인하시기바랍니다.

업데이트

업데이트는 V3 사용을 위한 가장 중요한 기능 중 하나입니다. 업데이트는 끊임없이 발견되는 악성코드와 알려지지 않은 보안 위협을 분석하여 새로운 악성코드와 보안 위협을 해결할 수 있는 기능을 가진 엔진 파일을 다운로드하는 기능입니다.

업데이트를 누르면, 안랩 업데이트 서버에 접속하여 최신 엔진 파일로 업데이트합니다.

업데이트 실행

업데이트를 실행하면 진행 상황을 표시합니다.

❖ 진행 비율: 업데이트 진행 비율을 표시합니다.

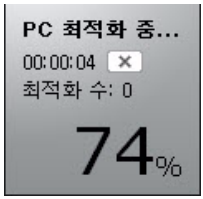
❖ 중지: 업데이트를 중지하고 싶은 경우에는 [×] 를 선택합니다.

PC 최적화

PC 최적화는 필요없는 임시 파일과 메모리를 정리하여 PC 사용과 인터넷 연결 개선에 도움이 됩니다.

PC 최적화 실행

PC 최적화를 실행하면 해당 영역이 다음과 같이 표시되면서 진행 상황을 표시합니다.



❖ 시간 표시 부분: PC 최적화 실행 후 경과한 시간을 표시합니다.

❖ 중지: 최적화를 중지하고 싶은 경우에는 ✕ 를 선택합니다.

❖ 최적화 수: 최적화한 대상의 개수를 표시합니다.

❖ 진행 비율: 빠른 검사 대상을 검사한 비율을 표시합니다.

참고

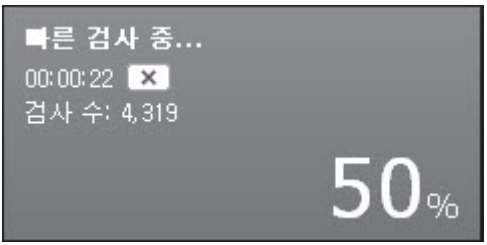
PC 최적화에 대한 자세한 내용은 PC 최적화를 참고하십시오.

빠른 검사

빠른 검사는 프로세스 영역, 부트 영역, 중요 시스템 영역과 같은 중요 폴더를 검사하는 기능입니다.

빠른 검사 실행

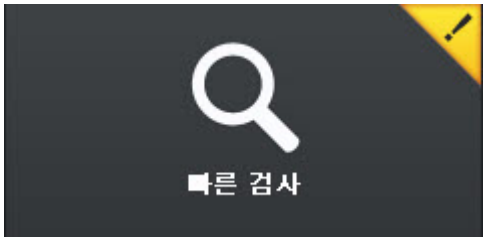
빠른 검사를 실행하면 해당 영역이 다음과 같이 표시되면서 진행 상황을 표시합니다.



- ❖ 시간 표시 부분: 빠른 검사 실행 후 경과한 시간을 표시합니다.
- ❖ 중지: 검사를 중지하고 싶은 경우에는 [×]를 선택합니다.
- ❖ 검사 수: 검사한 파일의 개수를표시합니다.
- ❖ 진행 비율: 빠른 검사를 진행한 비율을 표시합니다.

빠른 검사 실행 후 30일이 지난 경우

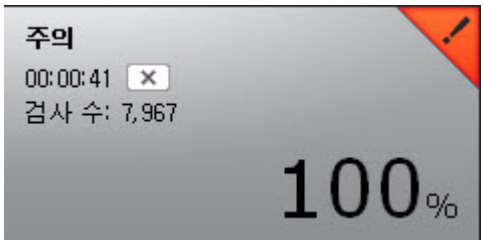
V3를 처음 설치했거나 빠른 검사를 실행한지 30일이 지난 경우에는 빠른 검사 영역의 아이콘이 다음과 같이 나타납니다.



❖ 빠른 검사를 눌러 PC를 검사하면 노란색의 주의 아이콘이 빠른 검사 영역에서 사라집니다.

빠른 검사에서 악성코드를 발견한 경우

빠른 검사에서 악성코드를 발견한 경우에는 빠른 검사 영역의 아이콘이 다음과 같이 나타납니다.



❖ 빠른 검사의 빨간색 아이콘을 누르면 치료 창이 나타납니다. 치료 창에서 치료하기를 눌러 감염된 파일을 치료합니다.

참고

치료 창에 대한 설명은 치료하기를 참고하십시오.


AhnLab

5장
보안 센터

화면 구성

보안 센터에서는 V3의 보안 기능 실행 여부에 따른 보안 상태를 종합적으로 확인할 수 있는 실시간 통계 정보를 제공합니다. 보안 센터를 활용하면 각 기능의 실행 여부와 기능별 상세 보기 정보를 통해 PC의 보안 상태를 더 안전하게 유지할 수 있습니다.

5

실행 방법

보안 센터를 실행하는 방법은 다음과 같습니다.

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **보안 센터** 탭을 선택합니다.

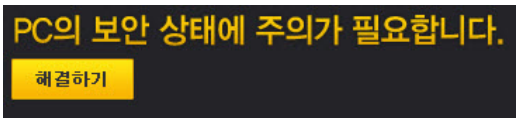
보안 센터 화면

A 영역

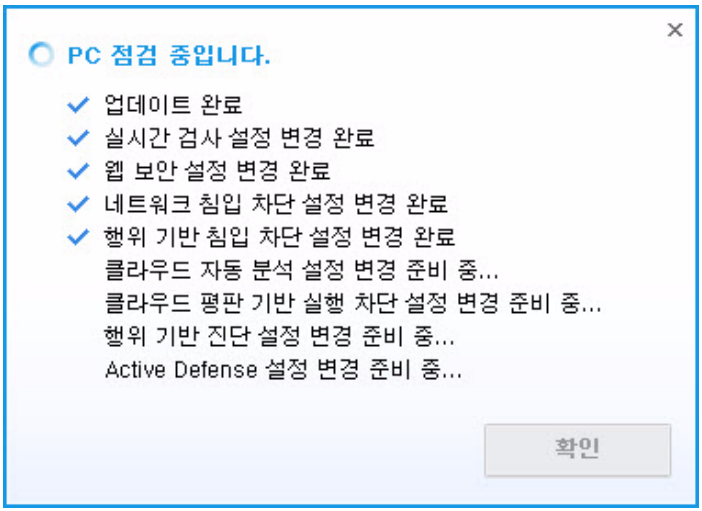
❖ PC의 보안 상태가 안전합니다.: 실시간 검사, 웹 보안, 클라우드 자동 분석 기능 등의 관련 기능이 모두 ON으로 설정된 경우입니다.

❖ PC의 보안 상태가 위험합니다.: 실시간 검사를 OFF로 설정한 경우입니다.

❖ PC의 보안 상태에 주의가 필요합니다.: 실시간 검사는 ON이지만, 웹 보안이나 클라우드 자동 분석 기능 등의 관련 기능 중 하나가 OFF로 설정된 경우입니다.



❖ 해결하기: 보안 상태가 위험이나 주의로 표시되는 경우 해결하기를 누르면 PC 점검을 실행하여 보안 상태를 안전한 상태로 설정합니다.



B 영역

- ❖ 최근 24시간 연결 PC: 최근 24시간 동안 ASD 네트워크에 참여한 PC의 개수를 표시합니다.
- ❖ 최근 24시간 위협 차단: 최근 24시간 동안 ASD 네트워크가 차단한 파일이나 사이트 등의 위협의 개수를 표시합니다.

C 영역

- ❖ ASD 클라우드 서버 현황: 안랩 클라우드 서버의 현황을 표시합니다.
- ❖ 유해 사이트: 안랩 클라우드 서버에 보고된 유해 사이트의 개수를 보여줍니다.
- ❖ 악성 파일: 안랩 클라우드 서버에 보고되어 악성 파일로 분류된 파일의 개수를 보여줍니다.
- ❖ 미확정 파일: 안랩 클라우드 서버에 보고되어 악성이나 정상으로 아직 분류되지 않은 미확정 파일에 대한 개수를 보여줍니다.

D 영역

각 보안 기능의 동작 여부를 표시하고, 각 보안 기능이 동작하면 해당 정보들을 실시간 수집하여 보여줍니다.

- ❖ 네트워크 보안: 네트워크 보안의 유해 사이트 차단, 네트워크 침입 차단, 행위 기반 침입 차단에 의해 발생한 정보를 실시간으로 보여줍니다.
- ❖ 클라우드 보안: 안랩 클라우드 관련 기능의 실행에 따라 검사한 파일의 개수와 차단한 파일의 개수를 실시간으로 보여줍니다.
- ❖ PC 보안: 엔진 업데이트 실행 여부, 악성코드 시그니처 정보, 검사 파일과 차단 파일에 대한 정보를 실시간으로 보여줍니다.
- ❖ 평판 기반 실행 차단: 평판 기반 실행 차단 관련 기능의 실행 여부와 해당 기능에 의해 탐지한 정보를 실시간으로 보여줍니다.
- ❖ 행위 기반 진단: 행위 기반 진단 관련 기능의 실행 여부와 해당 기능에 의해 탐지한 정보를 실시간으로 보여줍니다.
- ❖ Active Defense: Active Defense 관련 기능의 실행 여부와 해당 기능에 의해 신뢰하거나 탐지한 정보를 실시간으로 보여줍니다.

참고

각 항목에서 상세 보기를 누르면 해당 관련 기능의 실행 여부와 기능 동작에 따른 상세 정보를 확인할 수 있습니다.

참고

각 항목의 관련 기능이 모두 ON 상태인 경우에는 안전을 표시하는 파란색, 각 항목의 관련 기능 중 일부 기능이 OFF인 경우에는 위험이나 주의를 의미하는 주황색으로 표시됩니다.

상세 보기

보안 센터에 표시되는 각 항목의 상세 정보를 확인할 수 있습니다.

네트워크 보안

네트워크 보안을 담당하는 기능의 실행 여부를 표시하고 데이터 전송 상황, 각 기능에서 차단하거나 검사한 개수를 표시합니다.

- ❖ 유해 사이트 차단: 유해 사이트 차단 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 네트워크 침입 차단: 네트워크 침입 차단 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 행위 기반 침입 차단: 행위 기반 침입 차단 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 전송/수신 데이터: 네트워크를 통해 주고 받은 데이터의 송수신량을 표시합니다.
- ❖ 개인 방화벽 차단: 개인 방화벽 기능 작동 이후 개인 방화벽 규칙에 따라 차단한 개수를 표시합니다.
- ❖ 네트워크 침입 차단: 네트워크 침입 차단 기능 작동 이후 개인 방화벽 규칙에 따라 차단한 개수를 표시합니다.
- ❖ 유해 사이트 검사: 유해 사이트 차단 기능 작동 이후 유해 사이트를 검사한 개수를 표시합니다.
- ❖ 유해 사이트 차단: 유해 사이트 차단 기능 작동 이후 유해 사이트를 차단한 개수를 표시합니다.

클라우드 보안

클라우드 보안을 담당하는 기능의 실행 여부를 표시하고 검사 파일과 차단 파일의 개수를 표시합니다.

- ❖ PC 실시간 검사: PC 실시간 검사 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 클라우드 진단: 클라우드 진단 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 검사 파일: PC 실시간 검사와 클라우드 진단 기능 작동 이후 ASD 네트워크 검사를 실행한 개수입니다.

❖ 차단 파일: PC 실시간 검사와 클라우드 진단 기능 작동 이후 ASD 네트워크 검사에서 차단한 개수입니다.

PC 보안

악성코드를 진단하고 치료하는 PC 보안 담당 기능의 실행 여부와 엔진 업데이트 정보를 표시합니다.

❖ 최근에 엔진을 업데이트했습니다.: 최근 3일 이내에 엔진 업데이트를 실행한 경우입니다.

❖ 업데이트가 필요합니다.: 최근 3일 이내에 엔진 업데이트를 실행하지 않은 경우입니다.

❖ PC 실시간 검사: PC 실시간 검사 기능의 사용 여부를 ON/OFF로 표시합니다.

❖ 엔진 버전: 현재 사용 중인 엔진의 버전 정보를 표시합니다.

❖ 악성코드 시그니처: 현재 사용 중인 엔진에서 진단할 수 있는 악성코드의 개수입니다.

❖ 검사 파일: PC 실시간 검사 작동 이후 검사한 파일의 개수입니다.

❖ 차단 파일: PC 실시간 검사 작동 이후 차단한 악성 파일의 개수입니다.

평판 기반 실행 차단

클라우드 평판 기반 실행 차단을 담당하는 기능의 실행 여부와 탐지하여 차단한 파일의 개수를 표시합니다.

❖ PC 실시간 검사: PC 실시간 검사 기능의 사용 여부를 ON/OFF로 표시합니다.

❖ 클라우드 평판 기반 실행 차단: 클라우드 평판 기반 실행 차단 기능의 사용 여부를 ON/OFF로 표시합니다.

❖ 의심 파일 실행 탐지: 악성이 의심되는 파일의 실행을 탐지한 개수입니다.

❖ 허용: 클라우드 평판 기반 실행 차단 작동 이후 실행을 허용한 파일의 개수입니다.

❖ 차단: 클라우드 평판 기반 실행 차단 작동 이후 실행을 차단한 파일의 개수입니다.

행위 기반 진단

행위 기반 진단을 담당하는 기능의 실행 여부와 차단한 파일의 개수를 표시합니다.

- ❖ PC 실시간 검사: PC 실시간 검사 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 행위 기반 진단: 행위 기반 진단 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 의심 행위 차단: 행위 기반 진단 기능 작동 이후 탐지하여 차단한 악성 파일의 개수입니다.

Active Defense

Active Defense를 담당하는 기능의 실행 여부와 ASD 네트워크에 참여하는 사용자들이 신뢰하거나 차단한 파일에 대한 개수를 표시합니다.

- ❖ PC 실시간 검사: PC 실시간 검사 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ Active Defense: Active Defense 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 클라우드 자동 분석: Active Defense의 클라우드 자동 분석 기능의 사용 여부를 ON/OFF로 표시합니다.
- ❖ 미확정: ASD 네트워크에서 최근 7일간 발견된 파일 중 사용자가 신뢰나 차단을 선택하지 않은 파일의 개수입니다.
- ❖ 사용자 차단: ASD 네트워크에서 최근 7일간 발견된 파일 중 사용자들이 차단한 파일의 개수입니다.
- ❖ 사용자 신뢰: ASD 네트워크에서 최근 7일간 발견된 파일 중 사용자들이 신뢰한 파일의 개수입니다.

6장
빠른 검사

실행 방법

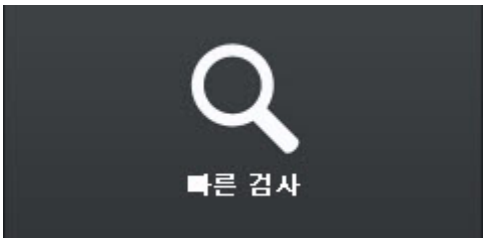
빠른 검사는 프로세스 영역, 부트 영역, 중요 시스템 영역과 같은 중요 폴더를 검사하는 기능입니다. 빠른 검사는 HOME 화면의 빠른 검사에서 실행하거나 작업 표시줄의 빠른 검사를 선택하여 실행할 수도 있습니다.

작업 표시줄에서 실행하기

❖ 작업 표시줄의 아이콘에서 마우스 오른쪽을 누르고 **빠른 검사**를 선택하면 실행할 수 있습니다.

HOME에서 실행하기

❖ V3 HOME 화면에서 빠른 검사를 누릅니다.



참고

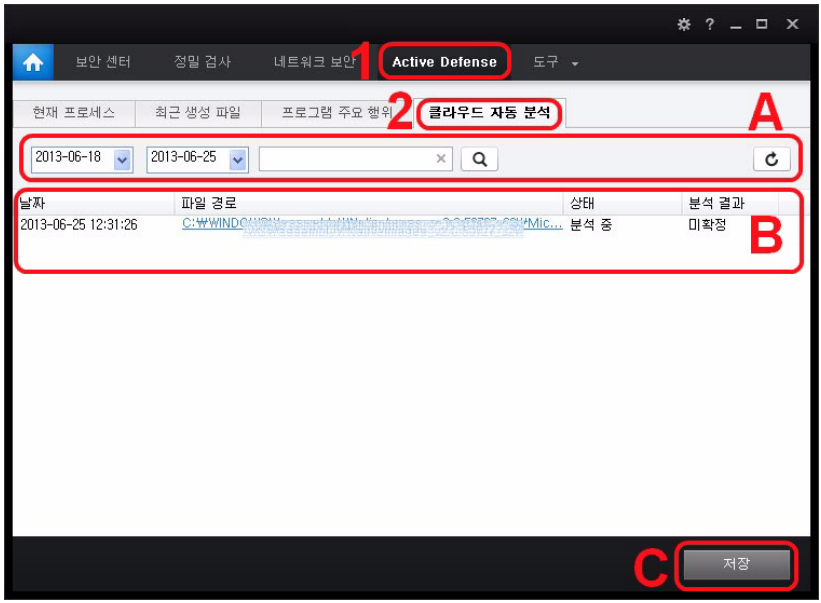
HOME에서 빠른 검사를 실행하면 HOME 화면 내에서 검사가 진행되며 빠른 검사의 검사 진행 화면이 표시되지 않습니다.

검사 진행 화면

작업 표시줄에서 빠른 검사를 선택하여 나타나는 검사 진행 화면에 대한 설명입니다.

빠른 검사 진행 화면

작업 표시줄에서 빠른 검사를 선택했을 때 나타나는 화면입니다.



A 영역

- ❖ 진행 비율: 검사 대상을 검사한 비율을 표시합니다.
- ❖ 일시 중지: 현재 검사를 잠시 중단합니다. 일시 중지를 누른 후 검사를 다시 하려면 다시 시작을 누릅니다.
- ❖ 다시 시작: 일시 중지를 누르면 일시 중지 버튼의 이름이 다시 시작으로 변경됩니다. 검사를 다시 시작할 수 있습니다.
- ❖ 검사 대상: 현재 검사하고 있는 대상을 보여줍니다.
- ❖ 검사 시간: 검사 실행 후 경과한 시간을 표시합니다.

❖ 검사 수: 검사한 파일의 개수를 표시합니다.

❖ 클라우드 자동 분석 요청: 안랩 클라우드 서버에 자동 분석을 요청한 파일의 개수를 표시합니다.

❖ 감염 수: 감염된 파일의 개수를 표시합니다.

❖ 치료 수: 감염된 파일 중 치료한 파일의 개수를 표시합니다.

B 영역

검사 중 발견된 악성코드에 대한 정보를 표시하는 영역입니다.

❖ 악성코드 이름: 감염된 악성코드의 이름을 보여줍니다.

❖ 상태: 감염 상태를 표시합니다. 감염 상태는 파일의 손상 정도에 따라 치료 가능 여부를 나타냅니다.

❖ 파일 경로: 감염된 파일이 실제 위치하고 있는 경로를 보여줍니다.

❖ 파일 분석 보고서: 감염된 파일에 대한 클라우드의 파일 분석 보고서로 연결합니다.

C 영역

검사 후 악성코드가 발견되지 않았을 경우 검사 창 처리 방법을 선택합니다.

❖ 악성코드가 발견되지 않으면 검사 창 그대로 두기: 검사 후 악성코드가 발견되지 않았을 경우 검사 창을 검사 종료 상태 그대로 둡니다.

❖ 악성코드가 발견되지 않으면 검사 창 닫기: 검사 후 악성코드가 발견되지 않았을 경우 검사 창을 닫습니다.

❖ 악성코드가 발견되지 않으면 PC 자동으로 끄기: 검사 후 악성코드가 발견되지 않았을 경우 PC를 종료합니다. 검사 실행 후 장시간 자리를 비워야 하는 경우에 활용하면 편리합니다.

D 영역

❖ 중지: 검사를 중지합니다. 중지를 누르면 현재 검사를 다시 시작할 수 없습니다.

❖ 마침: 검사를 끝냈거나 중지를 누른 경우 중지 버튼이 마침 버튼으로 변경됩니다. 마침을 누르면 현재 검사 창을 닫습니다.

7장
PC 실시간 검사

실행 방법

PC 실시간 검사는 메모리에 상주하여 사용자 PC에서 발생하는 파일의 복사, 이동, 실행, 다운로드 등의 일련의 행위를 검사하고 감염된 파일이 있는 경우 사용자가 설정한 치료 방법에 따라 처리하는 기능입니다. PC 실시간 검사는 악성코드가 PC에 유입되는 것을 차단할 수 있는 대표적인 기능입니다.

작업 표시줄에서 실행하기

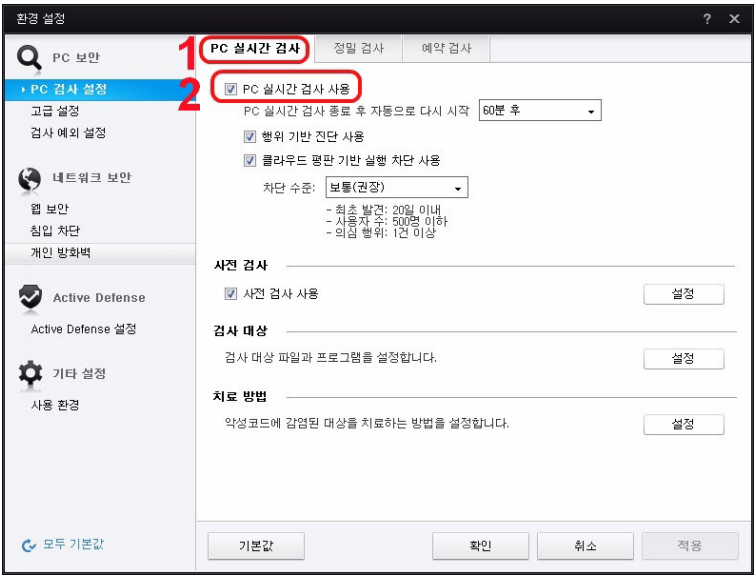
❖ 작업 표시줄의 아이콘에서 마우스 오른쪽을 누르고 PC 실시간 검사를 선택하면 실행할 수 있습니다.

보안 상태 설정에서 실행하기

❖ V3 HOME 화면의 보안 상태 설정을 선택하고, <보안 상태 설정>에서 PC 실시간 검사를 ON으로 설정합니다.

환경 설정에서 실행하기

❖ 환경 설정 실행 후 PC 검사 설정>PC 실시간 검사 탭을 선택하여 PC 실시간 검사 옵션을 선택할 수 있습니다.

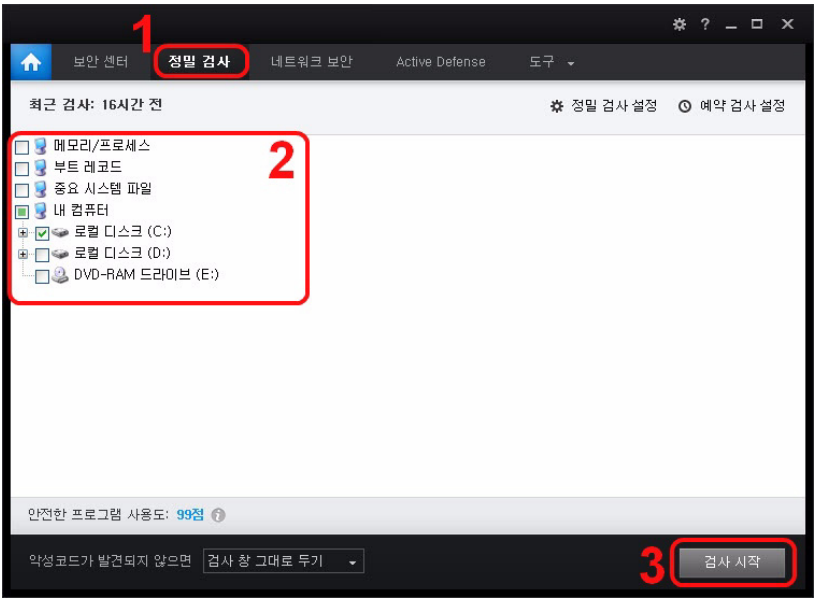


8장
정밀 검사

실행 방법

정밀 검사는 사용자가 선택한 검사 영역과 검사 대상을 검사하는 기능입니다. 정밀 검사는 PC 실시간 검사와 달리 V3 설치 이전에 감염된 파일을 검사할 수 있는 장점이 있지만, 선택한 파일의 개수와 종류에 따라 검사 시간이 오래 걸릴 수도 있습니다.

정밀 검사 실행 방법



1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3 HOME 화면에서 **고급 화면**을 선택합니다.

3 **정밀 검사** 탭을 누릅니다.

4 검사 영역을 선택합니다.

5 **검사 시작**을 누릅니다.

참고

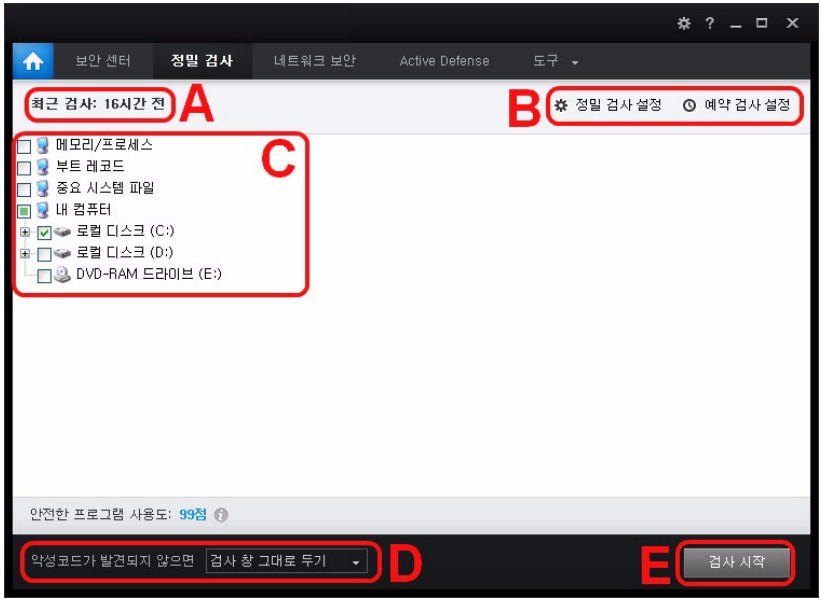
검사 영역에 대한 설명은 검사 선택 화면을 참고하십시오.

검사 선택 화면

정밀 검사를 선택했을 때 나타나는 화면에 대한 설명입니다.

정밀 검사 선택 화면

정밀 검사 선택 후 처음에 나타나는 화면입니다.



A 영역

❖ 최근 검사: 오늘 날짜를 기준으로 최근에 검사한 시간을 표시합니다. 몇 일전, 몇 시간전과 같은 형태로 나타납니다.

B 영역

❖ 정밀 검사 설정: 정밀 검사 탭으로 이동하여 정밀 검사에 대한 검사 대상과 치료 방법을 설정할 수 있습니다.

❖ 예약 검사 설정: 예약 검사 탭으로 이동하여 예약 검사 시간과 검사 대상, 치료 방법을 설정할 수 있습니다.

C 영역

검사 영역을 선택합니다.

- ❖ 메모리/프로세스: 메모리에 실행 중인 프로그램과 프로세스를 검사합니다.
- ❖ 부트 레코드: C 드라이브의 부트 레코드와 부팅한 드라이브의 부트 영역의 감염 여부를 검사합니다.
- ❖ 중요 시스템 파일: 시작 프로그램 폴더, 바탕 화면 폴더, Windows 설치 폴더와 같은 V3가 선정한 중요 시스템 파일에 대해 검사합니다.
- ❖ 내 컴퓨터: 로컬 디스크 (C:), DVD-RAM 드라이브(E:)와 같은 사용자 PC를 전체 선택하여 검사하거나 특정 로컬 디스크만 선택하여 검사합니다.

D 영역

검사 후 악성코드가 발견되지 않았을 경우 검사 창 처리 방법을 선택합니다.

- ❖ 악성코드가 발견되지 않으면 검사 창 그대로 두기: 검사 후 악성코드가 발견되지 않았을 경우 검사 창을 검사 종료 상태 그대로 둡니다.
- ❖ 악성코드가 발견되지 않으면 검사 창 닫기: 검사 후 악성코드가 발견되지 않았을 경우 검사 창을 닫습니다.
- ❖ 악성코드가 발견되지 않으면 PC 자동으로 끄기: 검사 후 악성코드가 발견되지 않았을 경우 PC를 종료합니다. 검사 실행 후 장시간 자리를 비워야 하는 경우에 활용하면 편리합니다.

E 영역

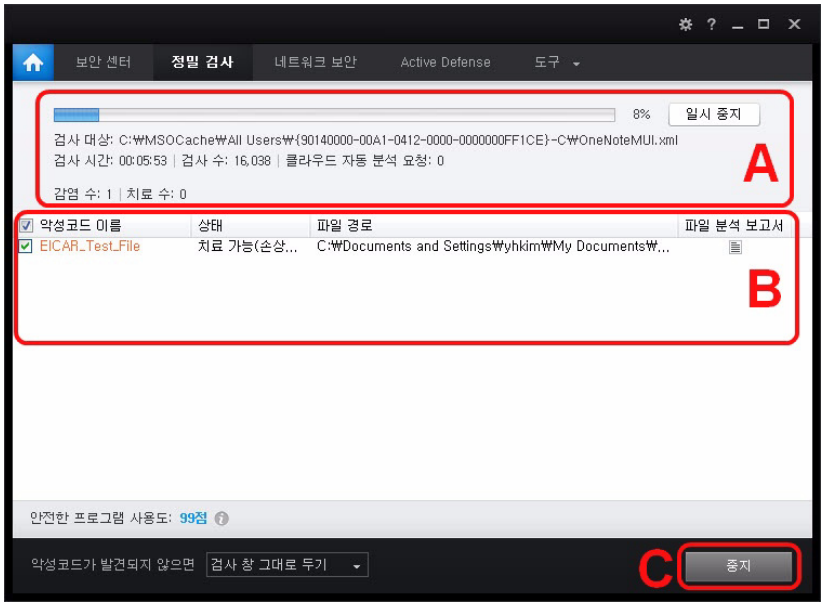
- ❖ 검사 시작: 선택한 내용에 따라 정밀 검사를 실행합니다. 검사 시작을 누르면 검사 진행 화면으로 화면이 변경됩니다.

검사 진행 화면

정밀 검사 선택 화면에서 검사 시작을 눌렀을 때 나타나는 검사 진행 화면에 대한 설명입니다.

정밀 검사 진행 화면

정밀 검사에서 검사 시작을 눌렀을 때 나타나는 화면입니다.



A 영역

- ❖ 진행 비율: 검사 대상을 검사한 비율을 표시합니다.
- ❖ 일시 중지: 현재 검사를 잠시 중단합니다. 일시 중지를 누른 후 검사를 다시 하려면 다시 시작을 누릅니다.
- ❖ 다시 시작: 일시 중지를 누르면 일시 중지 버튼의 이름이 다시 시작으로 변경됩니다. 검사를 다시 시작할 수 있습니다.
- ❖ 검사 대상: 현재 검사하고 있는 대상을 보여줍니다.
- ❖ 검사 시간: 검사 실행 후 경과한 시간을 표시합니다.

❖ 검사 수: 검사한 파일의 개수를 표시합니다.

❖ 클라우드 자동 분석 요청: 안랩 클라우드 서버에 자동 분석을 요청한 파일의 개수를 표시합니다.

❖ 감염 수: 감염된 파일의 개수를 표시합니다.

❖ 치료 수: 감염된 파일 중 치료한 파일의 개수를 표시합니다.

B 영역

검사 중 발견된 악성코드에 대한 정보를 표시하는 영역입니다.

❖ 악성코드 이름: 감염된 악성코드의 이름을 보여줍니다.

❖ 상태: 감염 상태를 표시합니다. 감염 상태는 파일의 손상 정도에 따라 치료 가능 여부를 나타냅니다.

❖ 파일 경로: 감염된 파일이 실제 위치하고 있는 경로를 보여줍니다.

❖ 파일 분석 보고서: 감염된 파일에 대한 클라우드의 파일 분석 보고서로 연결합니다.

C 영역

❖ 중지: 검사를 중지합니다. 중지를 누르면 현재 검사를 다시 시작할 수 없습니다.

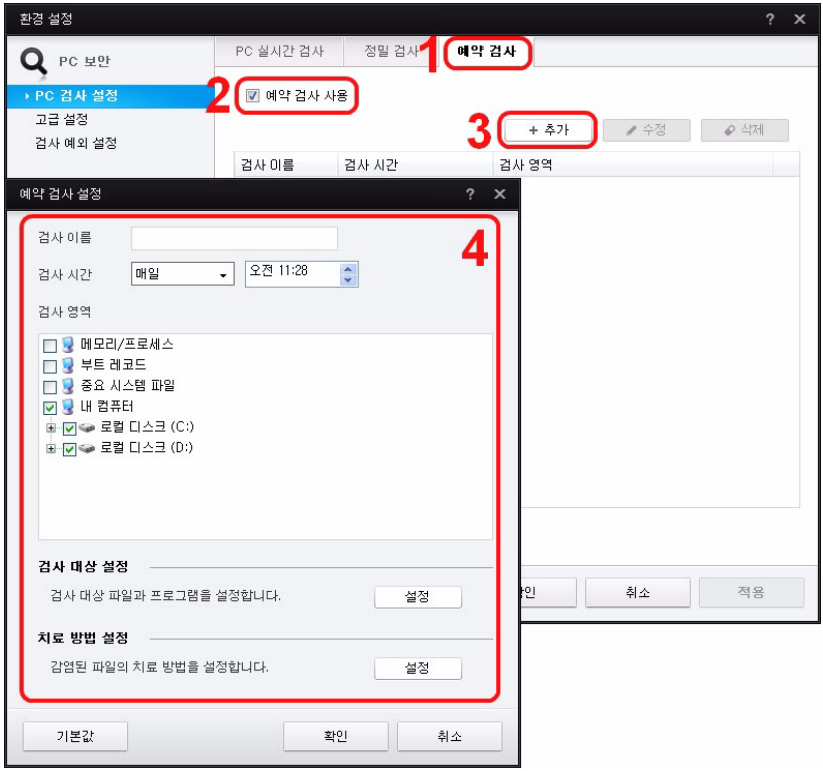
❖ 마침: 검사를 끝냈거나 중지를 누른 경우 중지 버튼이 마침 버튼으로 변경됩니다. 마침을 누르면 현재 검사 창을 닫습니다.

9장
예약 검사

실행 방법

예약 검사는 사용자가 설정한 시간에 정밀 검사를 자동으로 실행하는 기능입니다. 예약 검사는 환경 설정의 예약 검사에서 설정한 검사 주기에 PC를 검사합니다.

예약 검사 설정 방법



1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 화면 오른쪽 위에 있는 환경 설정 아이콘( )을 누릅니다.

3 **PC 보안>PC 검사 설정>예약 검사** 탭을 선택합니다.

4 **예약 검사 사용**을 선택합니다.

5 **추가**를 눌러 <예약 검사 설정>이 나타나면 검사 이름, 검사 시간, 검사 영역, 검사 대상, 치료 방법을 설정합니다.

참고

설정한 시간에 예약 검사가 진행되면, 작업 표시줄의 V3 아이콘이  로 변경됩니다.

참고

예약 검사 진행 화면에 대한 설명은 정밀 검사의 검사 진행 화면을 참고하십시오.

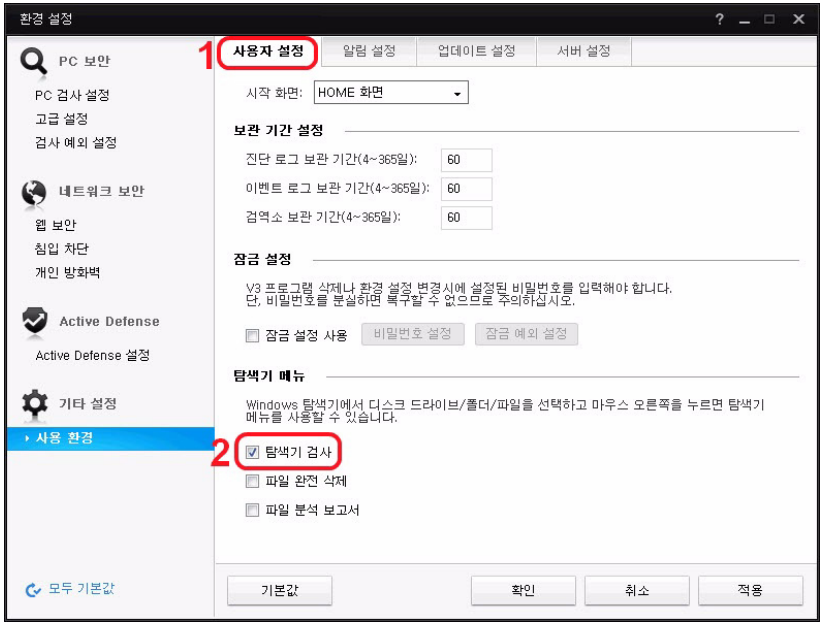

AhnLab

10장
탐색기 검사

실행 방법

탐색기 검사는 Windows 탐색기에서 사용자가 선택한 폴더나 대상을 탐색기에서 즉시 검사할 수 있는 기능입니다. 탐색기 검사를 실행하려면 환경 설정에서 탐색기 검사를 선택해야 합니다.

탐색기 검사 설정 방법



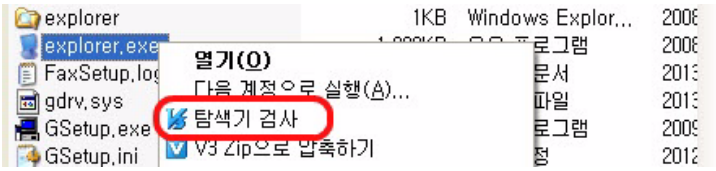
1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 화면 오른쪽 위에 있는 환경 설정 아이콘( )을 누릅니다.

3 **기타 설정>사용 환경>사용자 설정** 탭을 선택합니다.

4 **탐색기 검사**를 선택합니다.

탐색기 검사 실행 방법



1 바탕 화면이나 Windows 탐색기에서 폴더나 파일을 선택하고 마우스 오른쪽을 눌러 **V3 탐색기 검사**를 선택합니다.

2 탐색기 검사의 검사 진행 화면이 나타납니다.

참고

탐색기 검사 진행 화면에 대한 설명은 정밀 검사의 검사 진행 화면을 참고하십시오.

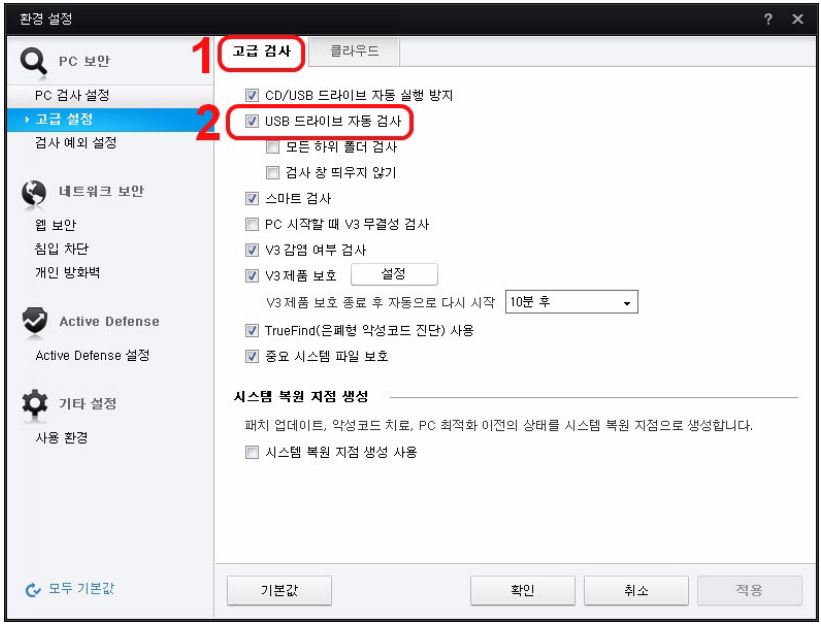

AhnLab

11장
USB 드라이브 검사

실행 방법

USB 드라이브 검사는 사용자 PC에 USB나 외장 하드와 같은 USB 미디어를 연결했을 때 자동 검사하는 기능입니다. USB 드라이브 검사를 사용하려면 환경 설정에서 USB 드라이브 자동 검사를 선택해야 합니다.

USB 드라이브 검사 설정 방법



1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 화면 오른쪽 위에 있는 환경 설정 아이콘( )을 누릅니다.

3 **고급 설정>고급 검사** 탭을 선택합니다.

4 **USB 드라이브 자동 검사**를 선택합니다.

USB 드라이브 검사 실행 방법

1 USB 드라이브에 USB 메모리나 외장 하드를 연결합니다.

2 USB 드라이브 검사 창에서 검사 진행 화면이 나타납니다.

참고

USB 드라이브 검사 진행 화면에 대한 설명은 정밀 검사의 검사 진행 화면을 참고하십시오.


AhnLab

12장
치료하기

치료하기

다양한 PC 검사를 통해 발견한 악성코드는 각 검사별로 설정한 치료 방법에 따라 치료합니다. 검사 진행 화면은 악성코드 발견 시 치료 화면으로 변경됩니다.

악성코드의 치료 방법

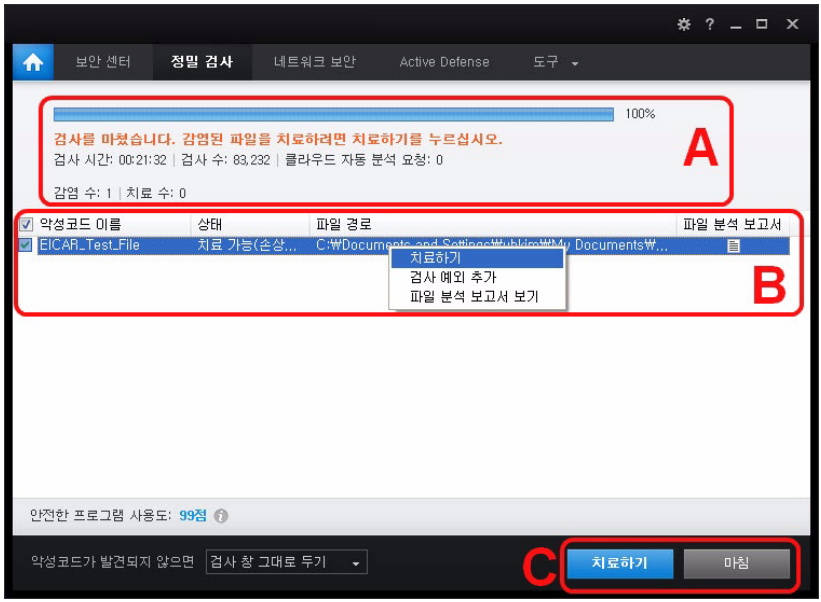
- ❖ PC 실시간 검사: 환경 설정>PC 검사 설정>PC 실시간 검사의 치료 방법에서 설정한 방법으로 치료합니다.
- ❖ 정밀 검사: 환경 설정>PC 검사 설정>정밀 검사의 치료 방법에서 설정한 방법으로 치료합니다.

참고

빠른 검사, 탐색기 검사, USB 드라이브 검사에서 악성코드를 발견한 경우에는 정밀 검사의 치료 방법에 따라 치료합니다.

- ❖ 예약 검사: 환경 설정>PC 검사 설정>예약 검사의 치료 방법에서 설정한 방법으로 치료합니다.

치료 화면



A 영역

- ❖ 진행 비율: 치료 대상을 치료한 비율을 표시합니다.
- ❖ 일시 중지: 현재 치료를 잠시 중단합니다. 일시 중지를 누른 후 치료를 다시 하려면 다시 시작을 누릅니다.
- ❖ 다시 시작: 일시 중지를 누르면 일시 중지 버튼의 이름이 다시 시작으로 변경됩니다. 치료를 다시 시작할 수 있습니다.
- ❖ 치료 대상: 현재 치료하고 있는 대상을 보여줍니다.
- ❖ 검사 시간: 검사 실행 후 경과한 시간을 표시합니다.
- ❖ 검사 수: 검사한 파일의 개수를 표시합니다.
- ❖ 클라우드 자동 분석 요청: 안랩 클라우드 서버에 자동 분석을 요청한 파일의 개수를 표시합니다.
- ❖ 감염 수: 감염된 파일의 개수를 표시합니다.
- ❖ 치료 수: 감염된 파일 중 치료한 파일의 개수를 표시합니다.

B 영역

검사 중 발견된 악성코드에 대한 정보를 표시하는 영역입니다.

- ❖ 악성코드 이름: 감염된 악성코드의 이름을 보여줍니다.
- ❖ 상태: 감염 상태를 표시합니다. 감염 상태는 파일의 손상 정도에 따라 치료 가능 여부를 나타냅니다.
- ❖ 파일 경로: 감염된 파일이 실제 위치하고 있는 경로를 보여줍니다.
- ❖ 파일 분석 보고서: 감염된 파일에 대한 클라우드의 파일 분석 보고서로 연결합니다.
- ❖ 치료하기: 감염된 파일을 치료합니다.
- ❖ 검사 예외 추가: 감염된 파일을 검사 예외 항목으로 추가합니다. 검사 예외 추가를 선택하면, **선택한 항목을 검사 예외 목록에 추가하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 검사 예외 목록에 추가후 치료하고, **아니오**를 누르면 검사 예외 목록에 추가하지 않고 치료합니다.
- ❖ 파일 분석 보고서 보기: 감염된 파일에 대한 클라우드의 파일 분석 보고서로 연결합니다.

C 영역

- ❖ 치료하기: 감염된 파일을 치료합니다.
- ❖ 마침: 치료 창을 닫습니다. 치료하지 않고 검사 창을 닫는 경우에는 치료되지 않은 파일이 있습니다. **치료를 마치지 않고 창을 닫으시겠습니까?** 라는 메시지가 나타납니다. 치료 창을 그냥 닫으려면 **예**를 선택하고, 다시 치료하려면 **아니오**를 눌러 감염된 파일을 치료합니다.

13장
네트워크 보안

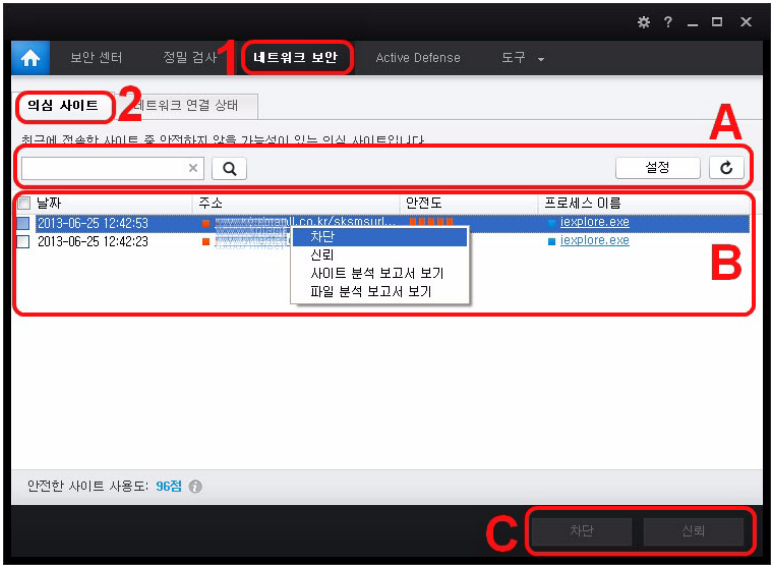
의심 사이트

의심 사이트는 사용자가 접속한 웹사이트 중 유해 사이트이거나 유해 사이트일 가능성이 있는 의심 사이트에 대한 목록을 표시하는 기능입니다. 의심 사이트 목록에 표시된 사이트 중 사용자가 해당 사이트를 선택하여 접속을 차단하거나 신뢰 사이트로 등록하여 관리할 수 있습니다.

실행 방법

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **네트워크 보안>의심 사이트** 탭을 선택하여 목록을 확인합니다.



의심 사이트 화면

A 영역

- ❖ 검색어 입력란: 의심 사이트 목록에서 사용자가 입력한 검색어와 일치하는 내용을 목록에 표시합니다.
- ❖ 설정: 환경 설정>네트워크 보안>웹 보안으로 연결합니다. 웹 보안 관련 기능을 설정할 수 있습니다.
- ❖ 새로 고침: 의심 사이트 목록을 최신 정보로 수정하여 표시합니다.

B 영역

- ❖ 날짜: 해당 사이트에 접속한 날짜와 시간입니다.
- ❖ 주소: 해당 사이트의 URL을 표시합니다.
- ❖ 안전도: 해당 사이트의 안전도를 표시합니다. 유해 사이트, 피싱 사이트, 불필요한 사이트로 알려진 사이트의 경우에는 위험을 표시하는 주황색의 막대가 표시되고, 안랩 클라우드 서버에 정보가 없는 사이트의 경우에는 회색으로 막대가 표시됩니다.
- ❖ 프로세스 이름: 현재 네트워크 연결을 하고 있는 프로세스의 이름입니다.
- ❖ 차단: 선택한 사이트를 사용자 지정 사이트 관리의 차단 사이트로 등록합니다. 차단을 선택하면, **선택한 항목을 환경 설정>네트워크 보안>웹 보안>사용자 지정 사이트 관리의 차단 사이트로 추가했습니다. 해당 사이트는 자동으로 차단됩니다.** 라는 메시지가 나타납니다. 차단 사이트로 지정되면 해당 사이트의 연결을 항상 차단합니다.
- ❖ 신뢰: 선택한 사이트를 사용자 지정 사이트 관리의 신뢰 사이트로 등록합니다. 신뢰를 선택하면, **선택한 항목을 환경 설정>네트워크 보안>웹 보안>사용자 지정 사이트 관리의 신뢰 사이트로 추가했습니다. 해당 사이트는 더 이상 의심 사이트 목록에 표시되지 않습니다.** 라는 메시지가 나타납니다. 신뢰 사이트로 지정되면 해당 사이트의 연결을 항상 허용합니다.
- ❖ 사이트 분석 보고서 보기: 웹브라우저를 이용하여 사이트 분석 보고서를 볼 수 있습니다. 사이트 분석 보고서에서는 사용자가 접근한 사이트에 대한 안전도 평가, 주요 행위, 해당 사이트에 대한 클라우드 정보를 확인할 수 있습니다.
- ❖ 파일 분석 보고서 보기: 웹브라우저를 이용하여 파일 분석 보고서를 볼 수 있습니다. 파일 분석 보고서에서는 해당 파일에 대한 안전도 평가, 클라우드의 파일 평판 정보를 확인할 수 있습니다.

C 영역

❖ 차단: 선택한 사이트를 사용자 지정 사이트 관리의 차단 사이트로 등록합니다. 차단을 선택하면, **선택한 항목을 환경 설정>네트워크 보안>웹 보안>사용자 지정 사이트 관리의 차단 사이트로 추가했습니다. 해당 사이트는 자동으로 차단됩니다.** 라는 메시지가 나타납니다. 차단 사이트로 지정되면 해당 사이트의 연결을 항상 차단합니다.

❖ 신뢰: 선택한 사이트를 사용자 지정 사이트 관리의 신뢰 사이트로 등록합니다. 신뢰를 선택하면, **선택한 항목을 환경 설정>네트워크 보안>웹 보안>사용자 지정 사이트 관리의 신뢰 사이트로 추가했습니다. 해당 사이트는 더 이상 의심 사이트 목록에 표시되지 않습니다.** 라는 메시지가 나타납니다. 신뢰 사이트로 지정되면 해당 사이트의 연결을 항상 허용합니다.

참고

의심 사이트 목록에서 차단하거나 신뢰할 사이트를 다음과 같이 선택하면 차단/신뢰 버튼이 활성화됩니다.

주의

신뢰 사이트로 추가하면, 해당 사이트가 유해 사이트인 경우에도 차단하지 않습니다. 유해 사이트에 계속 접속하면 해당 사이트를 통해 유포되는 악성코드에 감염될 위험이 있습니다.

13

알림 창

의심 사이트에 접속한 경우 알림 창이 표시됩니다. 의심 사이트 접속에 대한 알림 창이 표시되려면 다음과 같은 옵션이 선택되어 있어야 합니다.

❖ 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단 선택

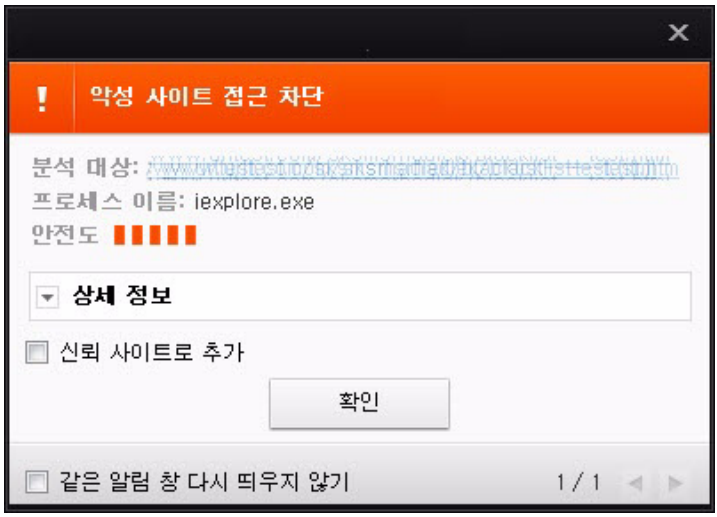
❖ 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단 선택>피싱 사이트 차단 선택

❖ 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단 선택>불필요한 사이트 차단 선택

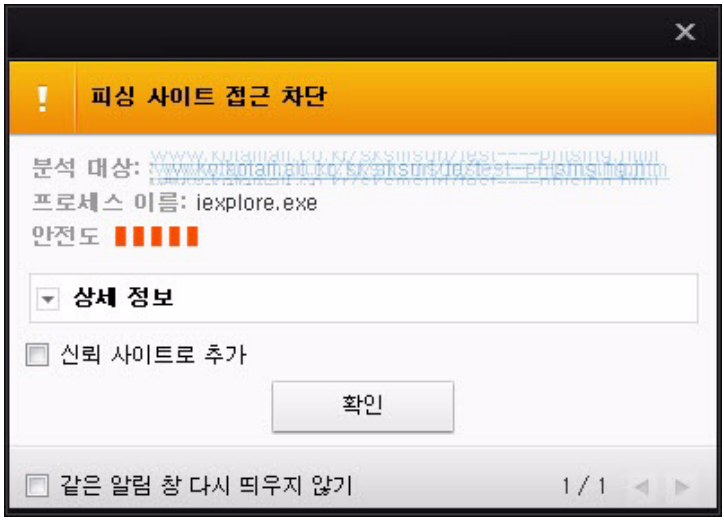
❖ 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단 선택>사용자 지정 사이트 관리>차단 추가에서 입력한 사이트

❖ 환경 설정>기타 설정>사용 환경>알림 설정>**선택한 상황에서 알림 창 표시** 선택>유해 사이트 차단 알림 선택

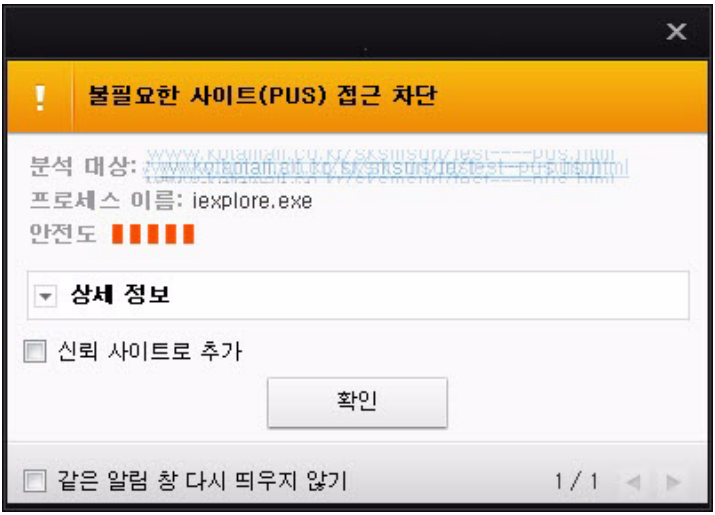
유해 사이트 차단 알림 창



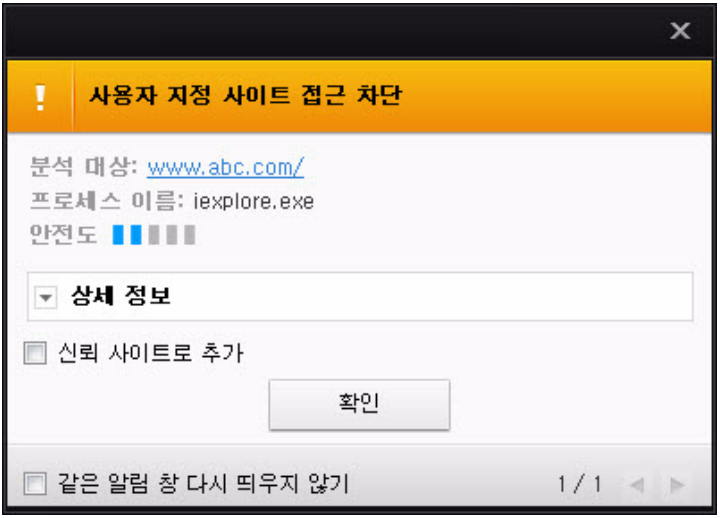
피싱 사이트 차단 알림 창



불필요한 사이트 차단 알림 창

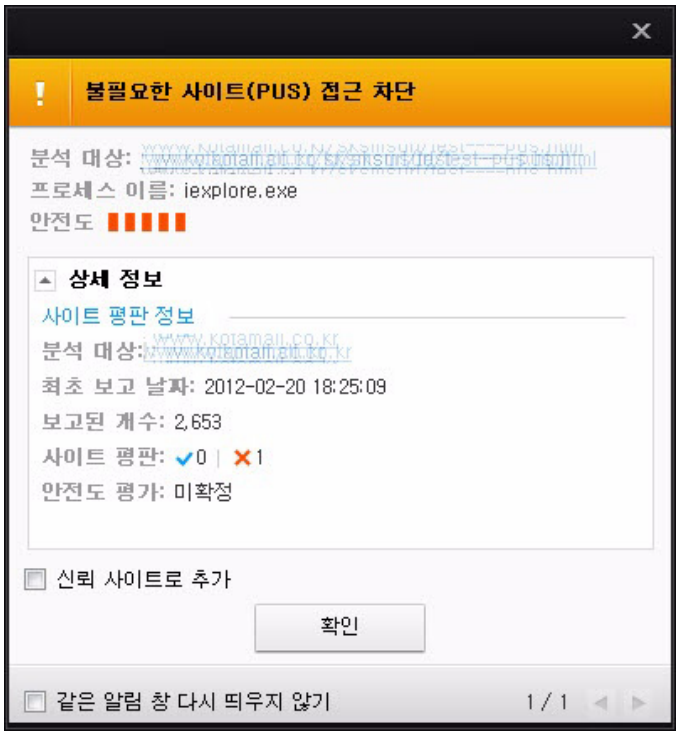


사용자 지정 사이트 관리의 차단 사이트 차단 알림 창



알림 창의 상세 정보

각 알림 창에서 상세 정보를 선택하면 접속한 사이트에 대한 클라우드 평판 정보 등의 상세 정보를 확인할 수 있습니다.



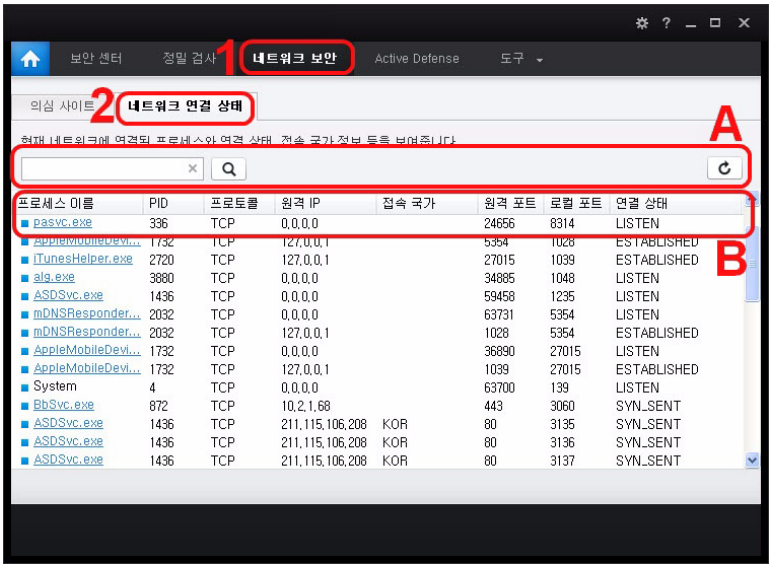
네트워크 연결 상태

네트워크 연결 상태는 현재 네트워크에 연결된 프로세스와 연결 상태, 접속 국가 정보 등을 보여줍니다. 네트워크 연결 상태는 네트워크 연결 상태를 V3 화면에서 보여주는 기능입니다. 네트워크 연결 상태의 접속 국가나 프로세스 이름을 확인하면, 위험 국가로 알려진 국가로의 접속이나 사용자가 실행하지 않은 프로세스가 네트워크 접속을 하는지를 파악하여 악의적인 연결이 있는지 파악하는데 도움이 될 수 있습니다.

실행 방법

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **네트워크 보안>네트워크 연결 상태** 탭을 선택하여 연결 상태를 확인합니다.



네트워크 연결 상태 화면

A 영역

- ❖ 검색어 입력란: 네트워크 연결 상태 목록에서 사용자가 입력한 검색어와 일치하는 내용을 목록에 표시합니다.
- ❖ 새로 고침: 네트워크 연결 상태 목록을 최신 정보로 수정하여 표시합니다.

B 영역

- ❖ 프로세스 이름: 현재 네트워크 연결을 하고 있는 프로세스의 이름입니다.
- ❖ PID: 특정 포트를 사용하는 프로그램의 PID(Page Identifier)입니다.
- ❖ 프로토콜: 연결에 사용한 프로토콜 이름입니다.
- ❖ 원격 IP: 접속 중인 원격지 IP 주소입니다.
- ❖ 접속 국가: 접속 중인 원격지 IP의 국가 정보입니다.
- ❖ 원격 포트: 접속 중인 원격지의 포트 번호입니다.
- ❖ 로컬 포트: 접속 중인 사용자 PC의 포트 번호입니다.
- ❖ 연결 상태: 네트워크 연결 상태입니다. 포트가 열려 있는 경우 LISTEN, 연결이 수립된 경우 ESTABLISH 등의 정보를 표시합니다.


AhnLab

14장
Active Defense

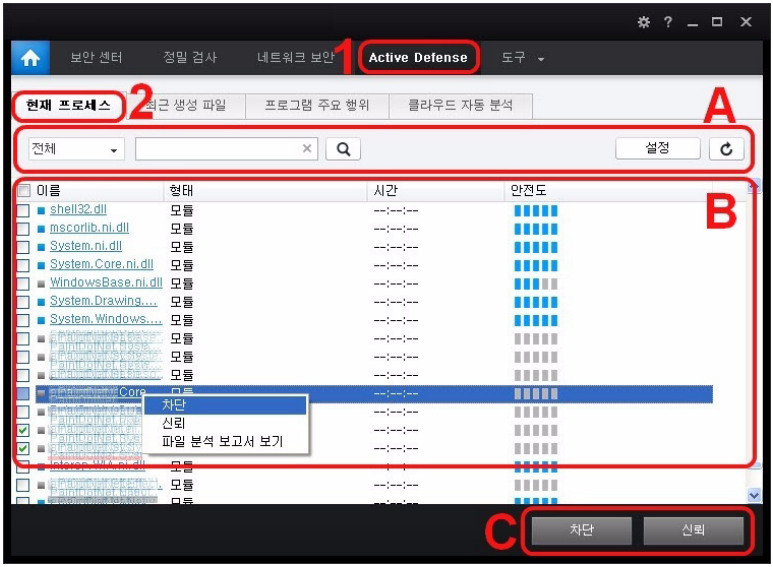
현재 프로세스

사용자 PC에서 현재 작동 중인 프로세스 중 의심 프로세스에 대해 필터링하여 보여줍니다. 현재 프로세스 목록에서 내용을 확인한 후 특정 프로세스를 선택하여 차단하거나 신뢰할 수 있습니다. 사용자들이 차단하거나 신뢰한 프로세스 정보는 안랩 클라우드 서버에 전송되어 클라우드 평판의 기초 자료로 활용됩니다.

실행 방법

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **Active Defense> 현재 프로세스** 탭을 선택하여 목록을 확인합니다.



현재 프로세스 화면

A 영역

- ❖ 악성: 현재 프로세스 목록을 표시하는 필터링의 조건으로 악성이거나 미확정으로 분류된 의심 프로세스를 표시합니다.
- ❖ 전체: 현재 실행 중인 모든 프로세스를 표시합니다.
- ❖ 검색어 입력란: 현재 프로세스 목록에서 사용자가 입력한 검색어와 일치하는 내용을 목록에 표시합니다.
- ❖ 설정: 환경 설정>Active Defense>Active Defense 설정으로 연결합니다. Active Defense 관련 기능을 설정할 수 있습니다.
- ❖ 새로 고침: 현재 프로세스 목록을 최신 정보로 수정하여 표시합니다.

B 영역

- ❖ 이름: 프로세스의 이름입니다.
- ❖ 형태: 실행 중인 프로세스의 파일 타입을 표시합니다. 모듈, 프로세스 등으로 나타납니다.
- ❖ 시간: 프로세스 실행 후 경과한 시간을 표시합니다.
- ❖ 안전도: 클라우드 서버의 평판 정보를 바탕으로 하여 안전, 주의, 위험 상태를 표시합니다.
- ❖ 차단: 현재 프로세스 목록에서 차단할 프로세스를 선택하고 차단을 누르면, 차단 프로세스로 등록됩니다. 차단 프로세스로 등록되면 해당 프로세스의 실행이 종료되고 프로세스의 실행 파일은 삭제됩니다. 이후에 PC 실시간 검사나 정밀 검사에서 차단 프로세스와 동일한 파일을 발견하면 해당 프로세스 관련 파일을 삭제합니다.
- ❖ 신뢰: 현재 프로세스 목록에서 신뢰할 프로세스를 선택하고 신뢰를 누르면, 신뢰 프로세스로 지정되어 해당 프로세스의 사용을 허용합니다.
- ❖ 파일 분석 보고서 보기: 웹브라우저를 이용하여 파일 분석 보고서를 볼 수 있습니다. 파일 분석 보고서에서는 해당 파일에 대한 안전도 평가, 클라우드의 파일 평판 정보를 확인할 수 있습니다.

참고

현재 프로세스 목록 화면에서 특정 프로세스를 선택하고 마우스를 더블 클릭하여 AhnLab V3 파일 분석 보고서를 확인할 수도 있습니다.

C 영역

- ❖ 차단: 현재 프로세스 목록에서 차단할 프로세스를 선택하고 차단을 누르면, 차단 프로세스로 등록됩니다. 차단 프로세스로 등록되면 해당 프로세스의 실행이 종료되고 프로세스의 실행 파일은 삭제됩니다. 이후에 PC 실시간 검사나 정밀 검사에서 차단 프로세스와 동일한 파일을 발견하면 해당 프로세스 관련 파일을 삭제합니다.
- ❖ 신뢰: 현재 프로세스 목록에서 신뢰할 프로세스를 선택하고 신뢰를 누르면, 신뢰 프로세스로 지정되어 해당 프로세스의 사용을 허용합니다.

참고

현재 프로세스 목록에서 차단하거나 신뢰할 프로세스를 다음과 같이 선택하면 차단/신뢰 버튼이 활성화됩니다.

의심 프로세스 판단 기준

V3는 다음과 같은 기준으로 의심 프로세스로 판단합니다.

- ❖ 검사 결과가 악성인 경우
- ❖ 안랩 클라우드 서버에 분석 정보가 없거나 안랩 인증서가 없는 경우
- ❖ 안랩 클라우드 서버에서 아직 분석 중이거나 안랩 인증서가 없는 경우
- ❖ 분석 결과가 미확정인 파일 중 안랩 인증서가 없고, 인증서 점수가 특정 기준 이하이고, 평판이 낮은 프로그램의 판단 기준에 해당하는 경우

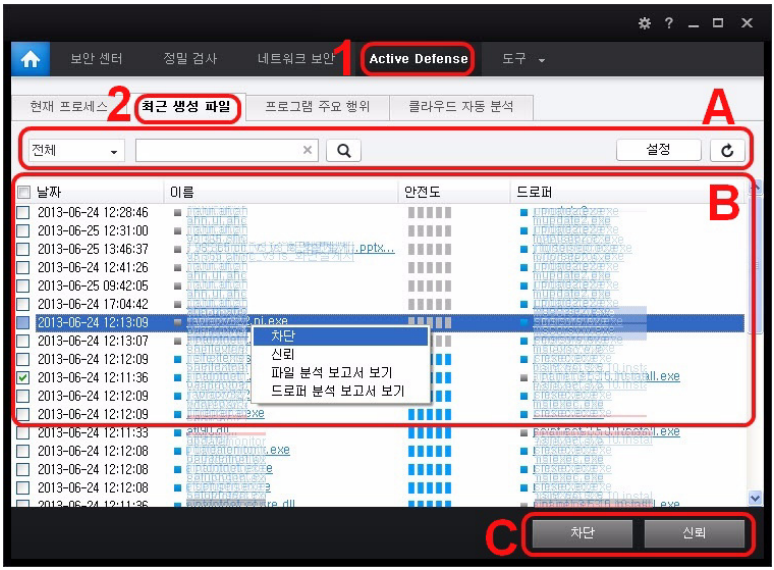
최근 생성 파일

최근 생성 파일에서는 최근 생성 파일 목록을 표시하고 의심 파일을 필터링하여 확인할 수 있는 기능입니다. 최근 생성 파일에서 내용을 확인한 후 특정 파일을 선택하여 차단하거나 신뢰할 수 있습니다. 사용자들이 차단하거나 신뢰한 파일에 대한 정보는 안랩 클라우드 서버에 전송되어 클라우드 평판의 기초 자료로 활용됩니다.

실행 방법

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **Active Defense> 최근 생성 파일** 탭을 선택하여 목록을 확인합니다.



최근 생성 파일 화면

A 영역

- ❖ 악성: 최근 생성 파일 목록을 표시하는 필터링의 조건으로 악성이거나 미확정으로 분류된 의심 파일을 표시합니다.
- ❖ 전체: 최근에 설치된 모든 파일을 표시합니다.
- ❖ 검색어 입력란: 최근 생성 파일 목록에서 사용자가 입력한 검색어와 일치하는 내용을 목록에 표시합니다.
- ❖ 설정: 환경 설정>Active Defense>Active Defense 설정으로 연결합니다. Active Defense 관련 기능을 설정할 수 있습니다.
- ❖ 새로 고침: 최근 프로세스 파일 목록을 최신 정보로 수정하여 표시합니다.

B 영역

- ❖ 날짜: 해당 파일이 생성된 날짜와 시간입니다.
- ❖ 이름: 파일의 이름입니다.
- ❖ 안전도: 클라우드 서버의 평판 정보를 바탕으로 하여 안전, 주의, 위험 상태를 표시합니다.
- ❖ 드로퍼: 파일을 생성한 프로세스 파일의 경로를 표시합니다.
- ❖ 차단: 최근 생성 파일 목록에서 차단할 파일을 선택하고 차단을 누르면, 차단 파일로 등록됩니다. 차단 파일로 등록되면 해당 파일은 삭제됩니다. 이후에 PC 실시간 검사나 정밀 검사에서 차단 파일과 동일한 파일을 발견하면 해당 파일을 삭제합니다.
- ❖ 신뢰: 최근 생성 파일 목록에서 신뢰할 파일를 선택하고 신뢰를 누르면, 신뢰 파일로 지정되어 해당 파일의 사용을 허용합니다.
- ❖ 파일 분석 보고서 보기: 웹브라우저를 이용하여 파일 분석 보고서를 볼 수 있습니다. 파일 분석 보고서에서는 해당 파일에 대한 안전도 평가, 클라우드의 파일 평판 정보를 확인할 수 있습니다.
- ❖ 드로퍼 분석 보고서 보기: 웹브라우저를 이용하여 파일 분석 보고서가 표시됩니다. 파일 분석 보고서의 Dropper 정보에서 드로퍼 정보를 확인할 수 있습니다.

참고

최근 생성 파일 목록 화면에서 특정 파일을 선택하고 마우스를 더블 클릭하면, AhnLab V3 파일 분석 보고서를 확인할 수 있습니다.

C 영역

❖ 차단: 최근 생성 파일 목록에서 차단할 파일을 선택하고 차단을 누르면, 차단 파일로 등록됩니다. 차단 파일로 등록되면 해당 파일은 삭제됩니다. 이후에 PC 실시간 검사나 정밀 검사에서 차단 파일과 동일한 파일을 발견하면 해당 파일을 삭제합니다.

❖ 신뢰: 최근 생성 파일 목록에서 신뢰할 파일를 선택하고 신뢰를 누르면, 신뢰 파일로 지정되어 해당 파일의 사용을 허용합니다.

참고

최근 생성 파일 목록에서 차단하거나 신뢰할 파일을 다음과 같이 선택하면 차단/신뢰 버튼이 활성화됩니다.

의심 파일 판단 기준

V3는 다음과 같은 기준으로 의심 파일로 판단합니다.

❖ 검사 결과가 악성인 경우

❖ 안랩 클라우드 서버에 분석 정보가 없거나 안랩 인증서가 없는 경우

❖ 안랩 클라우드 서버에서 아직 분석 중이거나 안랩 인증서가 없는 경우

❖ 분석 결과가 미확정인 파일 중 안랩 인증서가 없고, 인증서 점수가 특정 기준 이하이고, 평판이 낮은 프로그램의 판단 기준에 해당하는 경우

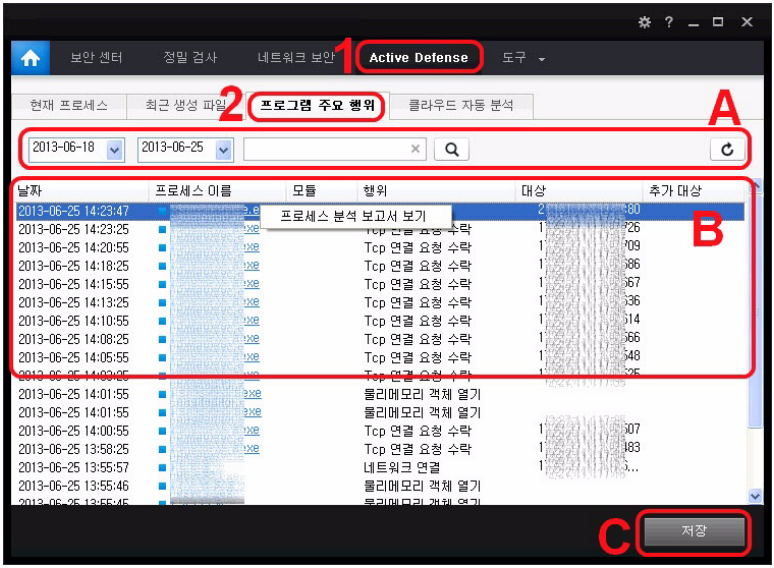
프로그램 주요 행위

프로그램 주요 행위에서는 PC에서 실행된 프로세스와 해당 프로세스가 실행한 작업 내역을 확인할 수 있습니다. 프로그램 주요 행위를 활용하면 PC에서 발생한 의심 행위에 대한 정보를 확인할 수 있어 악성 프로세스로 인한 피해를 예방하는데 도움이 됩니다.

실행 방법

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **Active Defense>프로그램 주요 행위** 탭을 선택하여 목록을 확인합니다.



프로그램 주요 행위 화면

A 영역

- ❖ 날짜 지정: 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- ❖ 검색어 입력란: 검색어를 입력할 수 있습니다.
- ❖ 검색 버튼: 검색 조건에 맞는 내용을 검색하여 화면에 표시합니다.
- ❖ 새로 고침: 프로그램 주요 행위 정보를 최신 정보로 고칩니다.

B 영역

- ❖ 날짜: 행위가 발생한 날짜와 시간입니다.
- ❖ 프로세스 이름: 행위를 발생시킨 프로세스의 이름입니다.
- ❖ 모듈: 행위를 발생시킨 프로세스와 관련 있는 모듈 이름입니다.
- ❖ 행위: 해당 프로세스의 행위 정보입니다.
- ❖ 대상: 행위를 발생시킨 목적이 되는 데이터의 정보입니다. 행위 유형에 따라 대상의 정보는 파일 이름, 모듈 이름, IP 주소 등이 표시됩니다.
- ❖ 추가 대상: 행위를 발생시킨 또 다른 목적이 되는 데이터의 정보입니다. 행위 유형에 따라 대상의 정보는 파일 이름, 모듈 이름, IP 주소 등이 표시됩니다.
- ❖ 프로세스 분석 보고서 보기: 웹브라우저를 이용하여 파일 분석 보고서가 표시됩니다. 파일 분석 보고서의 주요 행위에서 프로세스의 행위와 대상 정보를 확인할 수 있습니다.

C 영역

- ❖ 저장: 프로그램 주요 행위 목록의 내용을 CSV 파일 형태로 저장합니다. 저장을 누르면, 파일 이름과 저장 경로를 선택할 수 있습니다.

클라우드 자동 분석

안랩 클라우드 서버에 자동 분석을 요청한 파일에 대한 분석 상태와 분석 결과에 대한 정보를 확인할 수 있습니다.

실행 방법

1 V3 HOME 화면에서 **고급 화면**을 선택합니다.

2 고급 화면이 표시되면 **Active Defense>클라우드 자동 분석** 탭을 선택하여 목록을 확인합니다.

클라우드 자동 분석 화면

A 영역

❖ 날짜 지정: 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.

❖ 검색어 입력란: 검색어를 입력할 수 있습니다.

❖ 검색 버튼: 검색 조건에 맞는 내용을 검색하여 화면에 표시합니다.

❖ 새로 고침: 클라우드 자동 분석 결과를 최신 정보로 고칩니다.

B 영역

❖ 날짜: 분석을 요청한 날짜와 시간입니다.

❖ 파일 경로: 분석을 요청한 대상의 경로를 표시합니다.

❖ 상태: 분석 요청, 분석 중, 분석 완료로 구분하여 분석 진행 상황을 표시합니다.

❖ 분석 결과: 분석 결과를 정상, 악성, 미확정으로 구분하여 표시합니다.

- 정상: 클라우드 서버에 보고되어 분석 결과 악성코드에 감염되지 않은 정상 파일입니다.
- 악성: 클라우드 서버에 보고되어 분석 결과 악성코드에 감염된 파일입니다.
- 미확정: 클라우드 서버에 보고되었지만 정상과 악성 여부가 결정되지 않은 상태의 파일입니다.

C 영역

❖ 저장: 화면에 나타난 분석 요청 내용을 CSV 파일로 저장합니다.

참고

클라우드 자동 분석 목록 화면에서 특정 항목을 선택하고 마우스를 더블 클릭하면, AhnLab V3 파일 분석 보고서를 확인할 수 있습니다. 파일 분석 보고서에서는 파일에 대한 상세 정보와 클라우드 평판 정보를 확인할 수 있습니다.


AhnLab

15장
도구

PC 최적화

PC에서 사용하지 않는 시스템 정보를 삭제합니다. PC를 사용하면 많은 정보와 기록이 저장됩니다. 이러한 데이터들은 경우에 따라 다시 사용할 수도 있지만 대부분의 경우 삭제해도 PC 운영에 문제가 되지 않는 경우가 많습니다. 디스크 사용을 효율적으로 개선하고 PC 사용 속도와 메모리 사용을 개선하려면 PC 최적화를 실행하여 불필요한 공간 낭비를 최소화하는 것이 좋습니다.

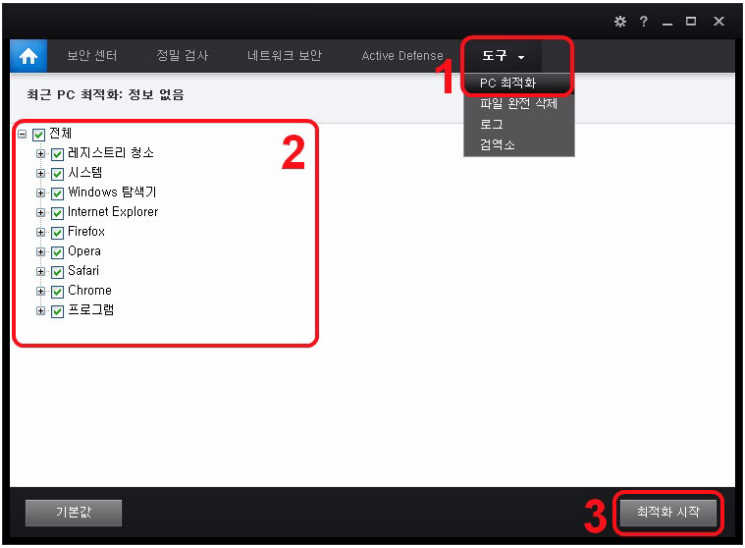
실행 방법

PC 최적화는 다양한 경로를 통해 실행할 수 있습니다.

참고

PC 최적화는 다양한 경로를 통해 실행할 수 있지만, 이미 다른 경로를 통해 PC 최적화가 진행 중인 경우에는 또 다른 경로를 통해 PC 최적화를 중복 실행할 수 없습니다.

도구에서 실행하기



1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 **도구>PC 최적화**를 누릅니다.

3 최적화 대상을 선택합니다.

4 **최적화 시작**을 누릅니다.

참고

최적화 대상에 대한 설명은 최적화 선택 화면을 참고하십시오.

HOME에서 실행하기

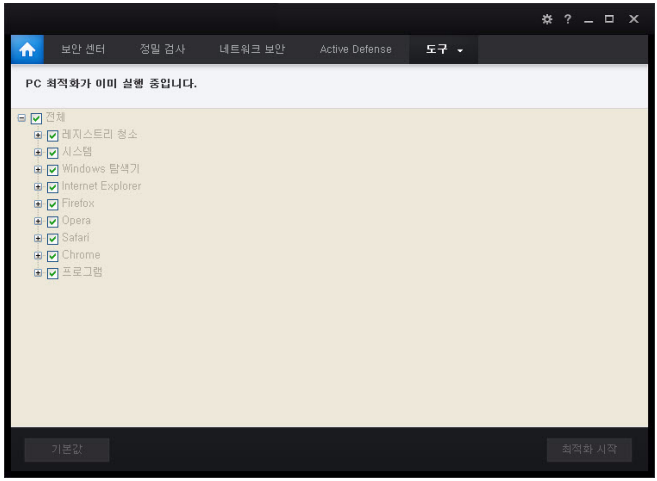
❖ V3 HOME 화면에서 PC 최적화를 누릅니다.

작업 표시줄에서 실행하기

❖ 작업 표시줄의 아이콘에서 마우스 오른쪽을 누르고 PC 최적화를 선택하면 실행할 수 있습니다.

PC 최적화를 중복 실행한 경우

PC 최적화는 다양한 경로에서 실행할 수 있지만, PC 최적화가 실행 중인 상태에서 다시 PC 최적화 탭을 누르면 다음과 같이 화면이 선택 불가 상태로 표시됩니다.

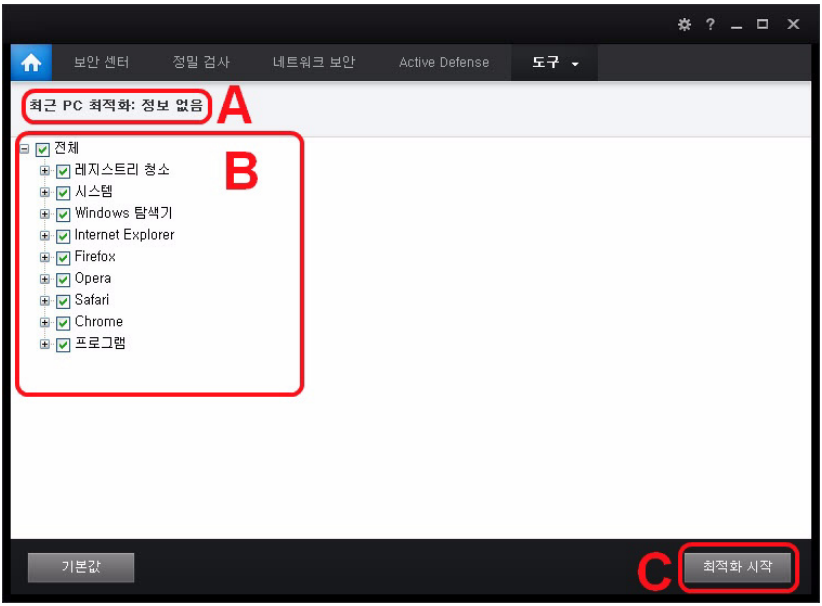


최적화 선택 화면

PC 최적화를 선택했을 때 나타나는 화면에 대한 설명입니다.

PC 최적화 선택 화면

PC 최적화 선택 후 처음에 나타나는 화면입니다.



A 영역

❖ 최근 PC 최적화: 오늘 날짜를 기준으로 최근에 최적화한 시간을 표시합니다. 조금 전, 몇 시간전, 몇 일전과 같은 형태로 나타납니다.

B 영역

최적화 대상을 선택할 수 있는 영역입니다.

전체

❖ 전체: 최적화 대상을 모두 선택하거나 선택을 모두 해제합니다.

레지스트리 청소

- ❖ 존재하지 않는 공유 DLL: 레지스트리에 공유 DLL의 경로가 잘못 저장되어 있을 경우 잘못된 정보로 인해 PC에 문제가 발생할 수 있습니다. 존재하지 않은 공유 DLL을 최적화 대상으로 선택하면 해당 공유 DLL의 레지스트리 정보를 삭제하여 PC 오류를 줄일 수 있습니다.
- ❖ 사용하지 않는 파일 확장자: 레지스트리에 등록된 확장자 정보를 제외한 빈 값으로 설정되어 있는 확장자 키 값을 모두 삭제합니다.
- ❖ ActiveX/COM 문제: ActiveX 레지스트리 정보 중 잘못되어 있거나 손상된 정보를 삭제합니다.
- ❖ 잘못된 타입 라이브러리: 레지스트리의 타입 라이브러리 키 값이 존재하지 않을 경우 키를 삭제합니다.
- ❖ 올바르지 않은 연결 프로그램: 레지스트리에 등록된 실행 파일의 경로가 유효하지 않을 경우 해당 키를 삭제합니다.
- ❖ 프로그램 경로: 실행했던 파일을 다음에 빨리 실행할 수 있도록 기록한 레지스트리를 삭제합니다.
- ❖ 도움말 파일: 레지스트리의 Windows Help 키 값에 정의된 파일 경로가 실제 존재하지 않을 경우 해당 키 값을 삭제합니다.
- ❖ 설치 프로그램 참조 문제: 프로그램 설치 시 만들어진 레지스트리 키 값으로 해당 키값에 정의된 디렉토리가 존재하지 않을 경우 키 값을 삭제합니다.
- ❖ 사용하지 않는 소프트웨어: 현재 사용하지 않는 소프트웨어의 정보를 삭제합니다.
- ❖ 시작 프로그램: Windows의 시작 프로그램으로 등록되어 있지만 실제로 시작 프로그램으로 사용하지 않거나 설치되지 않은 프로그램에 대한 키 값을 삭제합니다.
- ❖ 시작 메뉴 순서: Windows의 시작 버튼을 누르면, 설치한 프로그램이 이름 순서로 나타납니다. 이 순서 정보가 저장된 레지스트리를 삭제합니다.
- ❖ 존재하지 않는 MUI 참조: 프로그램이 사용하지 않는 지원 언어 정보를 삭제합니다.
- ❖ Windows 서비스: Windows 서비스와 관련된 레지스트리 키 값 중 사용하지 않는 키 값을 삭제합니다.

시스템

- ❖ 휴지통 비우기: 휴지통에 있는 모든 파일을 삭제합니다.
- ❖ 시스템 임시 파일: PC 사용 중 생성된 임시 파일을 삭제합니다.
- ❖ 클립보드: 클립보드 영역의 정보를 삭제합니다. 클립보드는 파일을 복사 또는 이동할 때 사용하는 임시 저장 영역입니다.
- ❖ 메모리 덤프: 메모리 덤프 정보를 삭제합니다. 메모리 덤프는 컴퓨터가 비정상적으로 종료되었을 때의 메모리 정보를 기록한 파일입니다.
- ❖ 디스크 검사 조각: 디스크 검사 후 생성된 디스크 검사 결과 파일을 삭제합니다.
- ❖ Windows 로그 파일: Windows 사용 중 기록된 로그를 삭제합니다.

Windows 탐색기

- ❖ 최근 문서: 시작 메뉴에 표시되는 최근 사용한 파일 목록을 삭제합니다. Windows에서 최근 문서 목록을 표시하도록 설정한 경우에 적용합니다.
- ❖ 시작 메뉴의 실행: 시작 메뉴에 표시되는 최근에 사용한 프로그램 목록을 삭제합니다. Windows에서 최근에 사용한 프로그램 목록을 표시하도록 설정한 경우에 적용합니다.
- ❖ 파일 검색: 파일을 검색한 내역을 삭제합니다.
- ❖ 컴퓨터 검색: 컴퓨터를 검색한 내역을 삭제합니다.
- ❖ 작업 표시줄 점프 목록: 작업 표시줄의 점프 목록에서 최근 항목을 삭제합니다.

Internet Explorer

- ❖ 임시 인터넷 파일: 임시 인터넷 파일을 삭제합니다. 임시 인터넷 파일을 사용하면 접속했던 웹페이지 및 미디어에 다시 접속할 때 속도는 빨라지지만 하드 디스크 공간을 많이 차지할 수 있습니다.
- ❖ 열어 본 페이지 목록: 접속했던 웹페이지의 목록을 삭제합니다.
- ❖ 쿠키: 쿠키를 삭제합니다. 쿠키는 사용자가 웹사이트를 이용한 내역을 저장한 정보입니다.
- ❖ 최근에 입력한 인터넷 주소: 최근에 입력했던 주소 목록을 삭제합니다.
- ❖ 인덱싱 파일: Internet Explorer를 사용한 모든 정보가 저장된 Index.dat 파일을 삭제합니다.

❖ 자동 완성: 자동 완성 기능에서 사용할 입력 값 정보를 삭제합니다. 자동 완성 기능을 사용하면 웹페이지의 입력 란에 기록했던 정보를 모두 저장합니다.

❖ 저장된 암호: 로그인할 때 저장한 암호를 삭제합니다. 저장된 암호를 사용하면 다음 로그인에는 암호를 입력하지 않아도 자동으로 로그인할 수 있지만 보안상 위험할 수 있습니다.

Firefox

❖ 캐시: 캐시를 삭제합니다. 캐시 정보를 사용하면 접속했던 웹페이지 및 미디어에 다시 접속할 때 속도는 빨라지지만 하드 디스크 공간을 많이 차지할 수 있습니다.

❖ 쿠키: 쿠키를 삭제합니다. 쿠키는 사용자가 웹사이트를 이용한 내역을 저장한 정보입니다.

❖ 방문 및 다운로드 기록: 방문한 웹사이트 기록과 파일을 다운로드한 내역을 삭제합니다.

❖ 세션: 세션 정보를 삭제합니다. 세션은 웹브라우저를 종료하기 직전에 사용하던 탭이나 창의 정보입니다.

❖ 웹사이트 설정: 특정 웹사이트에 접속할 때 사용하는 웹브라우저의 설정을 모두 삭제합니다.

❖ 폼 입력 및 검색 기록: 웹페이지의 입력란에 기록했던 정보를 모두 삭제합니다.

❖ 저장된 암호: 로그인할 때 저장한 암호를 삭제합니다. 저장된 암호를 사용하면 다음 로그인에는 암호를 입력하지 않아도 자동으로 로그인할 수 있지만 보안상 위험할 수 있습니다.

Opera

❖ 캐시: 캐시를 삭제합니다. 캐시 정보를 사용하면 접속했던 웹페이지 및 미디어에 다시 접속할 때 속도는 빨라지지만 하드 디스크 공간을 많이 차지할 수 있습니다.

❖ 방문 기록: 방문한 웹사이트 기록을 삭제합니다.

❖ 쿠키: 쿠키를 삭제합니다. 쿠키는 사용자가 웹사이트를 이용한 내역을 저장한 정보입니다.

❖ 최근 입력한 인터넷 주소: 최근에 입력했던 주소 목록을 삭제합니다.

❖ 세션: 세션 정보를 삭제합니다. 세션은 웹브라우저를 종료하기 직전에 사용하던 탭이나 창의 정보입니다.

❖ 웹사이트 아이콘: 접속했던 웹사이트의 아이콘 정보를 삭제합니다.

❖ 저장된 암호: 로그인할 때 저장한 암호를 삭제합니다. 저장된 암호를 사용하면 다음 로그인에는 암호를 입력하지 않아도 자동으로 로그인할 수 있지만 보안상 위험할 수 있습니다.

Safari

❖ 캐시: 캐시를 삭제합니다. 캐시 정보를 사용하면 접속했던 웹페이지 및 미디어에 다시 접속할 때 속도는 빨라지지만 하드 디스크 공간을 많이 차지할 수 있습니다.

❖ 방문 기록: 방문한 웹사이트 기록을 삭제합니다.

❖ 쿠키: 쿠키를 삭제합니다. 쿠키는 사용자가 웹사이트를 이용한 내역을 저장한 정보입니다.

Chrome

❖ 캐시: 캐시를 삭제합니다. 캐시 정보를 사용하면 접속했던 웹페이지 및 미디어에 다시 접속할 때 속도는 빨라지지만 하드 디스크 공간을 많이 차지할 수 있습니다.

❖ 인터넷 사용 정보: 인터넷을 사용할 때 기록된 모든 정보를 삭제합니다.

❖ 쿠키: 쿠키를 삭제합니다. 쿠키는 사용자가 웹사이트를 이용한 내역을 저장한 정보입니다.

❖ 세션: 세션 정보를 삭제합니다. 세션은 웹브라우저를 종료하기 직전에 사용하던 탭이나 창의 정보입니다.

❖ 저장된 암호: 로그인할 때 저장한 암호를 삭제합니다. 저장된 암호를 사용하면 다음 로그인에는 암호를 입력하지 않아도 자동으로 로그인할 수 있지만 보안상 위험할 수 있습니다.

프로그램

❖ Microsoft Office: Microsoft Office 제품 군에 해당하는 프로그램에서 최근에 사용한 파일 목록을 삭제합니다.

❖ Adobe Flash Player: 최근에 사용한 파일 목록을 삭제합니다.

❖ Microsoft Silverlight: 격리된 저장소의 파일 목록을 삭제합니다.

❖ QuickTime Player: 최근에 열었던 주소 및 파일 목록을 삭제합니다.

❖ Windows Media Player: 최근에 사용한 파일 목록을 삭제합니다.

C 영역

❖ 최적화 시작: 선택한 내용에 따라 최적화를 실행합니다. 최적화 시작을 누르면 최적화 진행 화면으로 화면이 변경됩니다.

최적화 진행 화면

최적화 선택 화면에서 최적화 시작을 눌렀을 때 나타나는 최적화 진행 화면에 대한 설명입니다.

PC 최적화 진행 화면

PC 최적화에서 최적화 시작을 눌렀을 때 나타나는 화면입니다.

A 영역

- ❖ 진행 비율: 최적화 대상에 대하여 최적화를 진행한 비율을 표시합니다.
- ❖ 진행 시간: 최적화를 실행한 후 경과한 시간을 표시합니다.
- ❖ 최적화 중입니다.: 최적화를 진행하고 있음을 알려줍니다. 최적화를 마친 경우에는 최적화를 마쳤습니다. 라고 표시됩니다.

B 영역

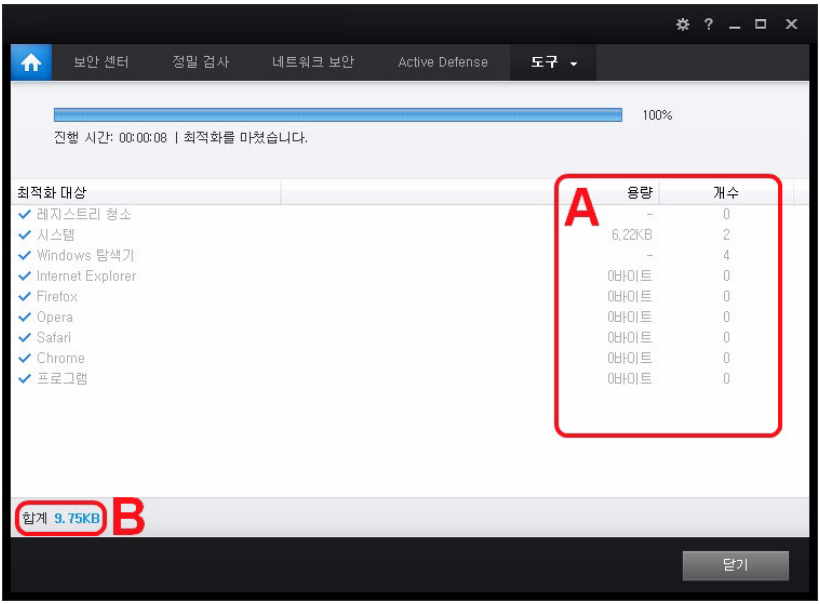
- ❖ 최적화 대상: 선택한 최적화 대상을 목록에 표시하며 최적화 대상 옆의 연두색 화살표는 현재 최적화하고 있는 대상을 가리킵니다.
- ❖ 용량: 최적화를 마친 후 최적화 후 확보한 용량을 표시합니다.
- ❖ 개수: 해당 최적화 대상에서 최적화한 대상의 개수를 표시합니다.

C 영역

- ❖ 중지: 현재 진행 중인 최적화를 중지합니다.

최적화를 마친 후의 화면

최적화를 마친 후에 나타나는 화면입니다.



A 영역

❖ 용량: 최적화 후 확보한 용량을 표시합니다.

❖ 개수: 해당 최적화 대상에서 최적화한 대상의 개수를 표시합니다.

B 영역

❖ 합계: 최적화로 확보한 전체 용량을 표시합니다.

파일 완전 삭제

파일 완전 삭제는 사용자가 선택한 파일이나 폴더를 완전히 삭제하여 복구 불가능한 상태로 삭제하는 기능입니다. 파일 완전 삭제는 불법 데이터 복구로 인해 개인 정보가 유출될 위험이 있는 파일이나 삭제 후 다시 사용할 필요가 전혀 없는 파일을 삭제하면 원치않는 복구로 인한 피해를 예방하는데 도움이 될 수 있습니다.

⚠ 주의

파일 완전 삭제를 실행하기 전에 대상 파일이 지워도 되는 파일인지 다시 한번 확인하십시오. 파일 완전 삭제는 파일에 관련된 정보를 복구 불가능한 상태로 모두 지웁니다. 따라서 삭제 후 필요에 의해 복구를 시도하면 복구를 할 수 없거나 원본 파일과 내용이 달라 다시 사용할 수 없으므로 반드시 확인하십시오.

실행 방법

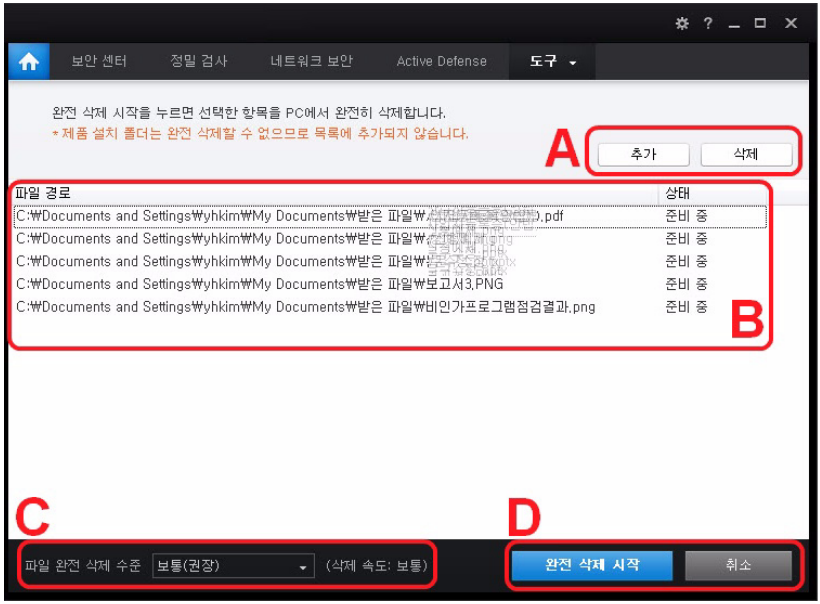
1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 **도구>파일 완전 삭제**를 누릅니다.

3 **추가**를 눌러 삭제 대상 파일을 선택합니다.

4 파일 완전 삭제 목록에 삭제 대상 파일이 표시되면 **완전 삭제 시작**을 누릅니다.

파일 완전 삭제 화면



A 영역

삭제 대상 파일을 추가하거나 목록에 추가한 파일을 목록에서 삭제할 수 있습니다.

❖ 추가: 삭제 대상 파일을 파일 완전 삭제 목록에 추가합니다. 추가를 누르면 파일 선택 창에서 대상 파일을 선택할 수 있습니다.

참고

바탕 화면이나 탐색기에서 삭제 대상 파일을 파일 완전 삭제 목록으로 끌어놓아도 파일 완전 삭제 대상으로 추가할 수 있습니다. 환경 설정의 탐색기 메뉴에서 파일 완전 삭제를 선택한 경우에는 삭제 대상 파일에서 마우스 오른쪽을 눌러 파일 완전 삭제를 즉시 실행할 수 있습니다.

❖ 삭제: 파일 완전 삭제 목록에 추가된 파일을 선택하고 삭제를 누르면 해당 파일을 삭제 목록에서 삭제합니다. 삭제를 누르면 **선택한 파일을 목록에서 삭제하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 파일을 목록에서 삭제합니다.

B 영역

❖ 파일 경로: 삭제 대상 파일의 경로와 파일 이름을 표시합니다.

❖ 상태: 파일 완전 시작 진행 상태를 표시합니다. 삭제 전인 경우 준비 중, 파일 완전 삭제를 마친 경우에는 성공으로 표시합니다.

C 영역

❖ 파일 완전 삭제 수준: 완전 삭제를 시작하기 전에 파일 완전 삭제 수준을 설정할 수 있습니다. 파일 완전 삭제 수준은 아주 높음, 높음, 보통(권장), 낮음, 아주 낮음을 선택할 수 있으며 기본값은 보통(권장)입니다. 파일 완전 수준에 따라 삭제 속도가 결정됩니다. 아주 높음인 경우의 삭제 속도는 아주 느림, 높음인 경우의 삭제 속도는 느림, 보통인 경우의 삭제 속도는 보통, 낮음인 경우의 삭제 속도는 빠름, 아주 낮음인 경우의 삭제 속도는 아주 빠름입니다.

❖ 완전 삭제 시작: 파일 완전 삭제 목록에 있는 파일을 완전 삭제합니다. 완전 삭제 시작을 누르면, **완전 삭제한 파일은 복원할 수 없습니다. 그래도 삭제하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 완전 삭제를 시작합니다.

❖ 취소: 파일 완전 삭제를 취소합니다. 삭제 목록에 파일을 추가한 상태에서 취소를 누르면, **삭제하지 않은 파일이 남아있습니다. 그래도 완전 삭제를 종료하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 파일 완전 삭제를 취소합니다.

❖ 마침: 파일 완전 삭제 시작을 실행하여 삭제를 마친 경우에는 취소 버튼이 마침으로 변경됩니다. 마침을 누르면, 파일 완전 삭제 초기 화면으로 돌아갑니다.

이벤트 로그

이벤트 로그는 V3의 각 기능을 실행한 기록을 보여줍니다. PC 검사, 네트워크 보안, 웹 보안, 도구 등을 실행한 기록과 작업 내역을 확인할 수 있습니다.

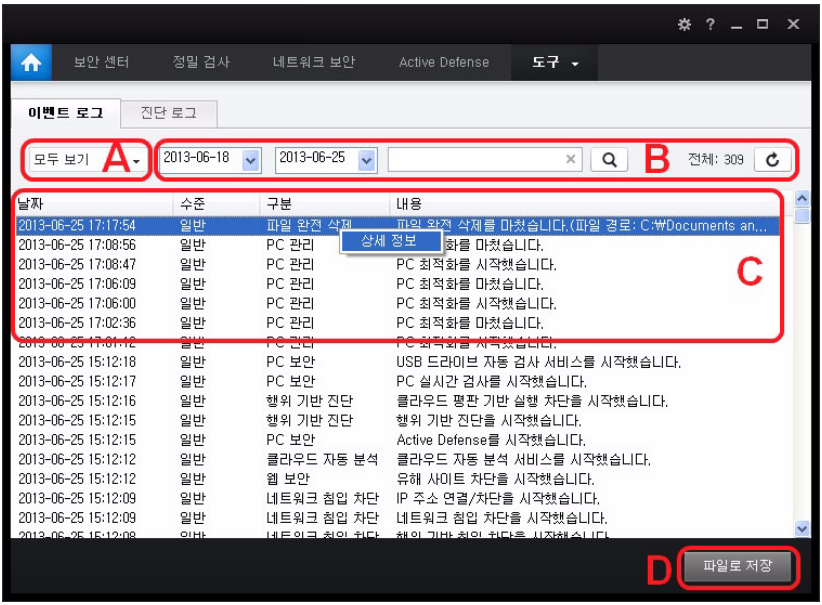
실행 방법

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 **도구>로그>이벤트 로그** 탭을 누릅니다.

3 이벤트 로그가 나타나면 로그 내용을 확인합니다.

이벤트 로그 화면



A 영역

이벤트 로그의 종류를 선택할 수 있습니다.

- ❖ 모두 보기: 모든 종류의 이벤트 로그를 보여줍니다.
- ❖ PC 보안: 빠른 검사, 정밀 검사, 예약 검사, USB 드라이브 검사, 실시간 검사와 같은 PC 검사를 실행한 기록을 보여줍니다.
- ❖ 네트워크 보안: 웹 보안의 유해 사이트 차단, 피싱 사이트 차단, 사용자 지정 사이트 관리, 네트워크 침입 차단, 행위 기반 침입 차단, 개인 방화벽을 실행한 기록을 보여줍니다.
- ❖ PC 관리: PC 최적화, 파일 완전 삭제를 실행한 기록을 보여줍니다.
- ❖ 기타: 업데이트와 ASD 서비스를 실행한 기록을 보여줍니다.

B 영역

이벤트 로그가 발생한 날짜를 선택할 수 있습니다.

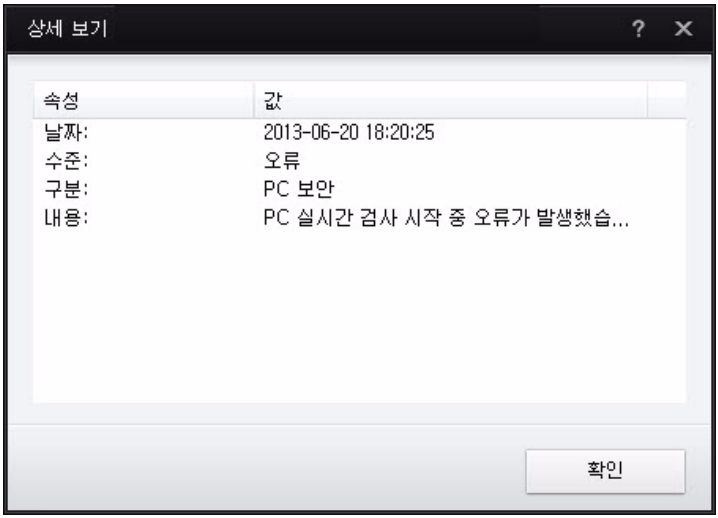
- ❖ 날짜 지정: 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- ❖ 검색어 입력란: 검색어를 입력할 수 있습니다.
- ❖ 검색 버튼: 이벤트 로그를 검색하여 화면에 표시합니다.
- ❖ 전체: V3에 저장된 이벤트 로그의 전체 개수를 표시합니다.
- ❖ 새로 고침: 이벤트 로그의 내용을 최신 정보로 고칩니다.

C 영역

검색 조건에 맞는 이벤트 로그의 내용을 표시합니다.

- ❖ 날짜: 이벤트가 발생한 날짜와 시간입니다.
- ❖ 수준: 이벤트 로그의 위험 수준을 표시합니다. 수준은 일반, 경고, 오류로 구분하여 나타납니다.
- ❖ 구분: 해당 이벤트가 발생한 기능 명칭이나 서비스 이름을 보여줍니다.
- ❖ 내용: 프로그램이나 서비스 시작과 종료 및 오류 내용을 보여줍니다.
- ❖ 상세 정보: 선택한 이벤트에 대한 상세 정보를 표시합니다.
  - 날짜: 해당 이벤트가 발생한 날짜와 시간입니다.
  - 수준: 일반과 오류로 구분하여 이벤트 수준을 표시합니다.
  - 구분: 이벤트가 발생한 모듈의 종류를 표시합니다.

- 내용: V3에서 실행한 작업 내용으로 이벤트 내용을 표시합니다.



D 영역

❖ 파일로 저장: 화면에 나타난 이벤트 로그의 내용을 CSV 파일로 저장합니다.

진단 로그

진단 로그는 사용자 PC에서 발견한 악성코드나 유해 사이트 차단에 대한 진단 날짜와 처리 상태를 확인할 수 있습니다.

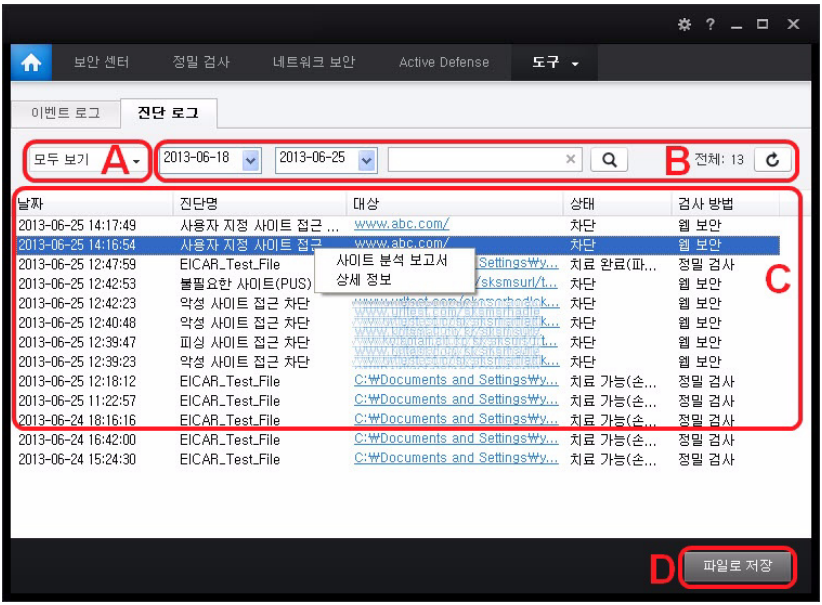
실행 방법

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 **도구>로그>진단 로그** 탭을 누릅니다.

3 진단 로그가 나타나면 로그 내용을 확인합니다.

진단 로그 화면



A 영역

진단 로그의 종류를 선택할 수 있습니다.

- ❖ 모두 보기: 모든 종류의 진단 로그를 보여줍니다.
- ❖ PC 보안: 빠른 검사, 정밀 검사, 예약 검사, USB 드라이브 검사, 실시간 검사와 같은 PC 검사를 통해 발견한 악성코드나 위협에 대한 정보를 보여주고 치료 상태를 보여줍니다.
- ❖ 네트워크 보안: 유해 사이트 차단, 피싱 사이트 차단, 사용자가 차단한 사이트, 네트워크 침입 차단, 행위 기반 침입 차단, 개인 방화벽에 대한 기록과 처리 상태를 보여줍니다.

B 영역

진단 로그가 발생한 날짜를 선택할 수 있습니다.

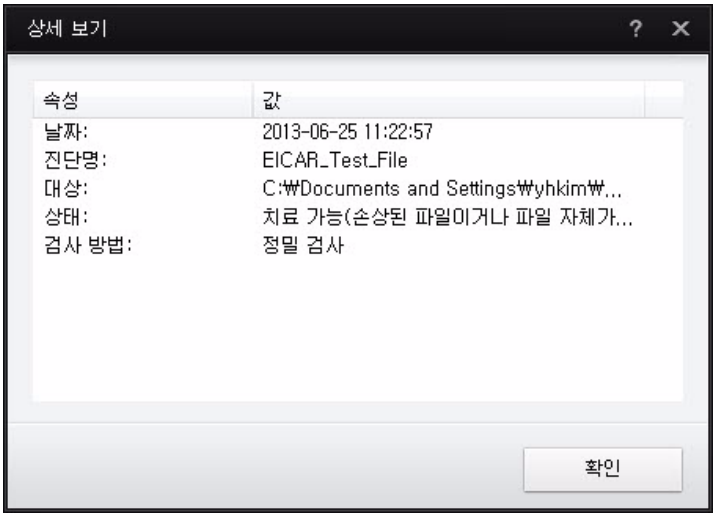
- ❖ 날짜 지정: 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- ❖ 검색어 입력란: 검색어를 입력할 수 있습니다.
- ❖ 검색 버튼: 진단 로그를 검색하여 화면에 표시합니다.
- ❖ 전체: V3에 저장된 진단 로그의 전체 개수를 표시합니다.
- ❖ 새로 고침: 진단 로그의 내용을 최신 정보로 고칩니다.

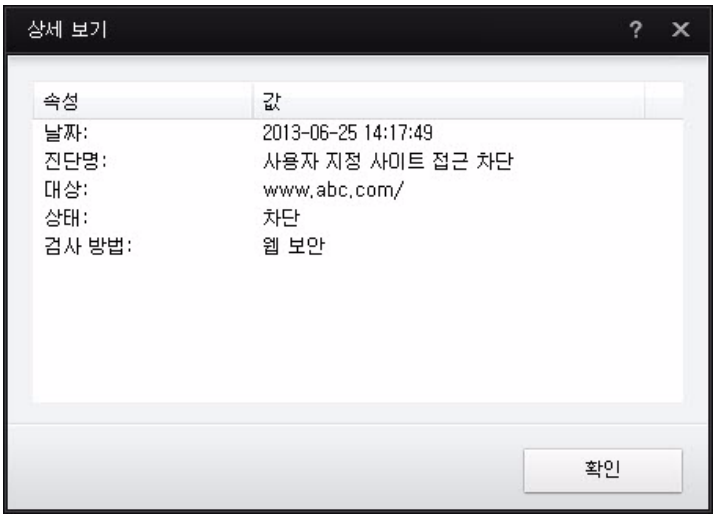
C 영역

검색 조건에 맞는 진단 로그의 내용을 표시합니다.

- ❖ 날짜: 진단 로그가 발생한 날짜와 시간입니다.
- ❖ 진단명: 감염된 악성코드의 이름이나 발견한 위협의 이름을 보여줍니다.
- ❖ 대상: 악성코드에 감염된 파일의 위치나 차단한 사이트의 주소를 표시합니다.
- ❖ 상태: 악성코드에 감염된 파일의 치료 상태나 사이트 차단 결과를 표시합니다.
- ❖ 검사 방법: 악성코드나 사이트를 차단한 V3의 기능 이름을 표시합니다.
- ❖ 파일 분석 보고서: 진단된 내용이 감염된 파일인 경우 해당 로그를 선택하고 마우스 오른쪽을 누르면 파일 분석 보고서를 선택할 수 있습니다. 파일 분석 보고서에서는 감염된 파일에 대한 상세 정보와 클라우드 평판 정보를 확인할 수 있습니다.
- ❖ 사이트 분석 보고서: 진단된 내용이 사이트인 경우 해당 로그를 선택하고 마우스 오른쪽을 누르면 사이트 분석 보고서를 선택할 수 있습니다. 사이트 분석 보고서에서는 해당 사이트에 대한 정보와 클라우드 평판 정보를 확인할 수 있습니다.
- ❖ 상세 정보: 선택한 파일이나 사이트에 대한 상세 정보를 표시합니다.
  - 날짜: 해당 파일이나 사이트를 진단한 날짜와 시간입니다.
  - 진단명: 파일인 경우 악성코드의 이름을 표시하고, 사이트인 경우에는 차단 종류를 표시합니다.
  - 대상: 파일인 경우 해당 파일의 실제 저장 경로를 표시하고, 사이트인 경우에는 사이트 주소를 표시합니다.
  - 상태: 파일인 경우 치료 가능 여부를 표시하고, 사이트인 경우에는 차단 여부를 표시합니다.

- 검사 방법: 파일인 경우에는 검사 방법을 표시하고, 사이트인 경우에는 차단한 모듈의 종류를 표시합니다.





D 영역

❖ 파일로 저장: 화면에 나타난 진단 로그의 내용을 CSV 파일로 저장합니다.

검역소

검역소는 악성코드에 감염된 파일을 치료하거나 삭제하기 전에 감염된 원본 파일이나 레지스트리 정보를 백업하는 기능입니다. 검역소는 악성코드 치료 이후 정상적으로 파일이 실행되지 않을 경우를 대비하여 감염된 상태이지만 치료 이전의 원본 파일이나 레지스트리를 보관하는 용도로 활용할 수 있습니다.

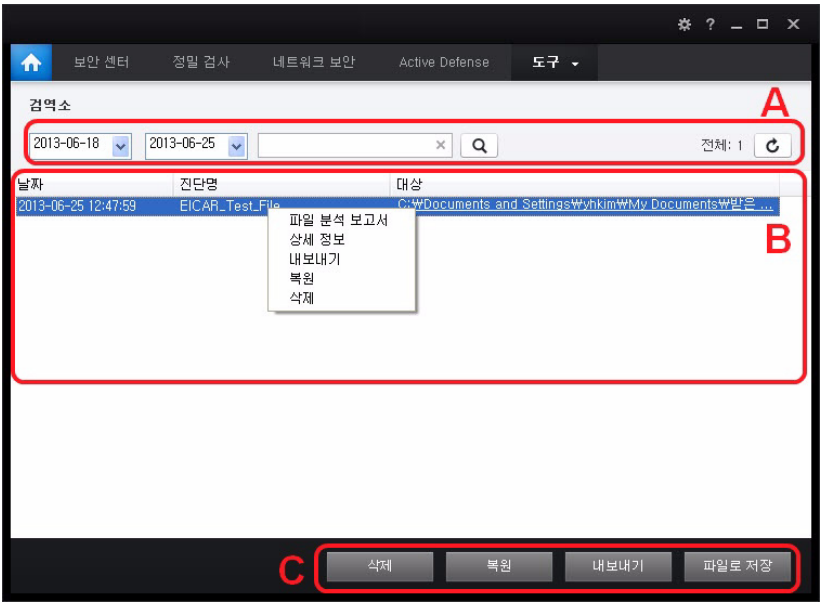
실행 방법

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 **도구>로그>검역소**를 선택합니다

3 검역소가 나타나면 내용을 확인합니다.

검역소 화면



A 영역

검역소에 백업한 날짜를 선택할 수 있습니다.

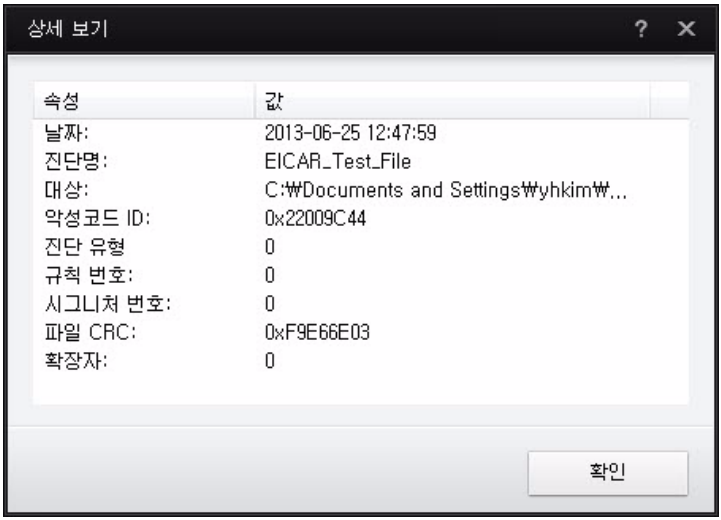
- ❖ 날짜 지정: 검색 날짜는 시작일과 종료일을 지정하여 검색할 수 있습니다.
- ❖ 검색어 입력란: 검색어를 입력할 수 있습니다.
- ❖ 검색 버튼: 검색 조건에 맞는 내용을 검색하여 화면에 표시합니다.
- ❖ 전체: 검역소에 백업된 파일의 전체 개수를 표시합니다.
- ❖ 새로 고침: 검역소의 내용을 최신 정보로 고칩니다.

B 영역

검색 조건에 맞는 검역소의 내용을 표시합니다.

- ❖ 날짜: 검역소에 백업한 날짜와 시간입니다.
- ❖ 진단명: 검역소에 백업된 파일이나 레지스트리에 감염된 악성코드의 이름이나 발견한 위협의 이름을 보여줍니다.
- ❖ 대상: 악성코드에 감염된 파일이나 레지스트리의 원본 위치를 표시합니다.
- ❖ 파일 분석 보고서: 백업된 내용이 파일인 경우 해당 내용을 선택하고 마우스 오른쪽을 누르면 파일 분석 보고서를 선택할 수 있습니다. 파일 분석 보고서에서는 감염된 파일에 대한 상세 정보와 클라우드 평판 정보를 확인할 수 있습니다.

❖ 상세 정보: 선택한 백업 파일에 대한 자세한 정보를 확인할 수 있습니다.



- 날짜: 검역소에 파일을 백업한 날짜와 시간입니다.
- 진단명: 검역소에 백업된 파일이 감염된 악성코드의 이름이나 위협의 이름입니다.
- 대상: 감염된 파일의 원본 위치를 표시합니다.
- 악성코드 ID: 안랩에서 정의한 악성코드의 ID입니다.
- 진단 유형: 악성코드나 위협을 발견한 검사 방법을 표시합니다.
- 규칙 번호: 시그니처의 규칙 번호를 표시합니다.
- 시그니처 번호: 검사/치료 엔진에 포함된 시그니처의 번호입니다.
- 파일 CRC: 파일의 CRC 값을 표시합니다.
- 확장자: 파일의 포맷 정보를 표시합니다.

❖ 삭제: 검역소에 백업된 파일이나 레지스트리를 검역소에서 삭제합니다.

❖ 복원: 검역소에 백업된 파일이나 레지스트리를 원래 폴더로 복원합니다. 복원을 누르면, **복원하는 파일이나 레지스트리를 검사 예외 목록에 추가하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 검사 예외 목록에 추가후 복원하고, **아니오**를 누르면 검사 예외 목록에 추가하지 않고 복원합니다.

❖ 내보내기: 검역소에 백업된 파일이나 레지스트리를 다른 폴더로 복원합니다. **복원하는 파일이나 레지스트리를 검사 예외 목록에 추가하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 복원할 위치를 지정한 후 검사 예외 목록에 추가하여 복원하고, **아니오**를 누르면 복원할 위치만 지정합니다.

참고

상세 정보에 표시되는 값들은 악성코드에 대한 내부 정보를 포함하고 있고 해당 내용의 값을 코드로만 표시합니다.

C 영역

❖ 삭제: 검역소에 백업된 파일이나 레지스트리를 검역소에서 삭제합니다.

❖ 복원: 검역소에 백업된 파일이나 레지스트리를 원래 폴더로 복원합니다. 복원을 누르면, **복원하는 파일이나 레지스트리를 검사 예외 목록에 추가하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 검사 예외 목록에 추가후 복원하고, **아니오**를 누르면 검사 예외 목록에 추가하지 않고 복원합니다.

❖ 내보내기: 검역소에 백업된 파일이나 레지스트리를 다른 폴더로 복원합니다. **복원하는 파일이나 레지스트리를 검사 예외 목록에 추가하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 복원할 위치를 지정한 후 검사 예외 목록에 추가하여 복원하고, **아니오**를 누르면 복원할 위치만 지정합니다.

❖ 파일로 저장: 화면에 나타난 검역소 내용을 CSV 파일로 저장합니다.


AhnLab

16장
분석 보고서

파일 분석 보고서

파일 분석 보고서는 PC 검사에서 발견한 파일이나 클라우드 서버에 자동 분석 요청을 의뢰한 파일에 대한 정보를 확인할 수 있는 기능입니다. 파일 분석 보고서를 활용하면, 진단된 파일에 대한 기본 정보와 클라우드 평판 정보를 참고할 수 있습니다.

참고

인터넷이 정상 실행되지 않는 환경에서는 클라우드 정보가 파일 분석 보고서에 표시되지 않을 수도 있습니다.

파일 분석 보고서 실행 방법

파일 분석 보고서를 실행할 수 있는 방법은 다음과 같습니다.

- ❖ 감염된 파일이 발견된 경우: 치료 창에서 감염된 파일을 선택하고 마우스 오른쪽 버튼을 눌러 **파일 분석 보고서**를 선택합니다.
- ❖ 진단 로그에서 확인하기: 도구>로그의 진단 로그를 실행한 후 로그 내용 중 감염된 파일을 선택하고 마우스 오른쪽 버튼을 눌러 **파일 분석 보고서**를 선택합니다.
- ❖ 검역소에서 확인하기: 도구>검역소를 실행한 후 검역소 목록 중 감염된 파일을 선택하고 마우스 오른쪽 버튼을 눌러 **파일 분석 보고서**를 선택합니다.
- ❖ 클라우드 자동 분석에서 확인하기: Active Defense>클라우드 자동 분석을 실행한 후 목록 중 감염된 파일을 선택하고 마우스 오른쪽 버튼을 눌러 **파일 분석 보고서**를 선택합니다.
- ❖ 네트워크 보안에서 확인하기: 네트워크 보안>의심 사이트에서 의심 사이트 목록에 표시된 항목을 선택하고 마우스 오른쪽 버튼을 눌러 **파일 분석 보고서**를 선택합니다.
- ❖ 탐색기에서 확인하기: 환경 설정>사용 환경>사용자 설정의 탐색기 메뉴에서 파일 분석 보고서를 선택한 경우 탐색기에서 파일을 선택하고 마우스 오른쪽을 누르고 **파일 분석 보고서**를 선택합니다.

참고

파일 분석 보고서는 Internet Explorer와 같은 웹 브라우저에 파일 분석 보고서의 내용이 나타납니다.

파일 분석 보고서의 내용

❖ 요약 정보: 요약 정보에서는 사용자 PC에서 발견한 파일에 대한 간단한 정보를 제공합니다. 요약 정보에서는 최초 발견 날짜, 의심 행위 개수, 디지털 서명, 제작자, 최초 실행 날짜, 유포 경로를 확인할 수 있습니다.

❖ 클라우드 평판 정보: 클라우드 평판 정보는 안랩 클라우드 서버에 저장된 해당 파일에 대한 정보를 보여줍니다. 클라우드 평판 정보에서는 다운로드 주소, 안랩 클라우드 서버에 해당 파일이 최초 보고된 최초 보고 날짜, 해당 파일을 사용하고 있는 사용자 수, 클라우드 평판, 최초 발견 국가, 안전도 평가를 확인할 수 있습니다. 안전도 평가는 악성, 정상, 의심, 불필요한 프로그램(PUP)로 표시합니다.

❖ 발견 파일 정보: 사용자 PC에서 발견한 파일에 대한 정보를 제공합니다. 파일 이름, 파일 경로, 파일 크기, 만든 날짜, 수정한 날짜, 액세스한 날짜, 최초 발견 날짜, 최초 실행 날짜, MD5 정보를 표시합니다.

❖ 버전 정보: 사용자 PC에서 발견한 파일에 대한 버전 정보를 제공합니다. 파일 설명, 제작사, 설명, 파일 버전, 내부 이름, 저작권, Legal Trademarks, 원본 파일 이름, 제품 이름, 제품 버전, Private Build, Special Build, 언어, Codepage 정보를 표시합니다.

❖ 디지털 서명: 사용자 PC에서 발견한 파일에 대한 디지털 서명 정보를 제공합니다. 서명자 이름, 연대 서명자 이름 , 타임 스탬프, 정상 여부를 표시합니다. 디지털 서명의 정상 여부는 인증서가 정상인 경우 **정상 인증서**, 인증서가 올바르지 않은 경우 **비정상 인증서**로 표시합니다.

❖ MS Catalog: 선택한 파일이 Windows 시스템 파일과 같이 Microsoft의 인증이 필요한 파일인 경우 파일의 인증 여부를 표시하여 정상 여부를 표시합니다. 정상인 경우 **인증**, 정상이 아닌 경우 **미인증**으로 표시합니다.

❖ 의심 행위 이력: 사용자 PC에서 발견한 파일의 의심 행위에 대한 클라우드 정보를 제공합니다.

❖ Dropper 정보: Dropper 정보를 표시합니다. 날짜, 파일 이름, 제작사, 클라우드 평판을 확인할 수 있습니다.

보고서의 저장과 인쇄

파일 분석 보고서를 PC에 저장하거나 인쇄하려면, 보고서를 보여주는 웹 브라우저의 저장과 인쇄 기능을 활용하면 됩니다.

참고

본 설명에서는 Internet Explorer를 기준으로 설명합니다.

❖ 저장: 파일 분석 보고서가 표시된 Internet Explorer의 **파일>다른 이름으로 저장**을 선택합니다. <웹 페이지 저장>이 나타나면 파일을 저장한 위치와 파일 이름을 설정합니다.

❖ 인쇄: 파일 분석 보고서가 표시된 Internet Explorer의 **파일>인쇄**를 선택합니다.

사이트 분석 보고서

사이트 분석 보고서는 접속한 사이트 중 유해 사이트로 차단된 사이트에 대한 정보를 확인할 수 있는 기능입니다.

참고
인터넷이 정상 실행되지 않는 환경에서는 사이트 분석 보고서의 일부 정보와 클라우드 정보가 표시되지 않을 수도 있습니다.

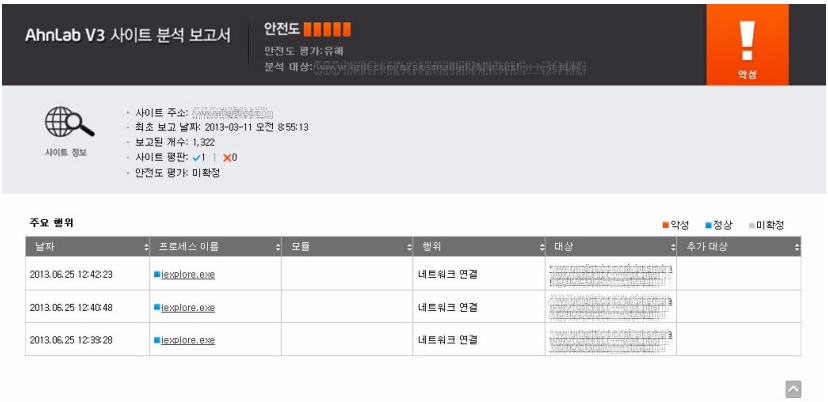
사이트 분석 보고서 실행 방법

사이트 분석 보고서를 실행할 수 있는 방법은 다음과 같습니다.

- ❖ 진단 로그에서 확인하기: 도구>로그의 진단 로그를 실행한 후 로그 내용 중 차단된 사이트를 선택하고 마우스 오른쪽 버튼을 눌러 **사이트 분석 보고서**를 선택합니다.
- ❖ 네트워크 보안에서 확인하기: 네트워크 보안>의심 사이트에서 의심 사이트 목록에 표시된 항목을 선택하고 마우스 오른쪽 버튼을 눌러 **사이트 분석 보고서**를 선택합니다.

참고
사이트 분석 보고서는 Internet Explorer와 같은 웹 브라우저에 사이트 분석 보고서의 내용이 나타납니다.

사이트 분석 보고서의 내용



❖ 사이트 정보: 사이트 정보에서는 해당 사이트가 클라우드에 최초 보고된 날짜, 보고된 개수, 사이트 평판 정보, 안전도 평가를 확인할 수 있습니다.

❖ 사이트 접속 차단 이력: 접속한 사이트에 대한 차단 기록을 보여줍니다. 차단한 날짜, 사이트 주소, 포트 번호, 프로그램, 파일 결과를 확인할 수 있습니다.

❖ 주요 행위: 주요 행위에서는 해당 사이트에서 발견한 행위에 대한 정보를 보여줍니다. 날짜, 프로세스 이름, 모듈, 행위, 대상, 추가 대상을 확인할 수 있습니다.

보고서의 저장과 인쇄

사이트 분석 보고서를 PC에 저장하거나 인쇄하려면, 보고서를 보여주는 웹 브라우저의 저장과 인쇄 기능을 활용하면 됩니다.

참고

본 설명에서는 Internet Explorer를 기준으로 설명합니다.

❖ 저장: 사이트 분석 보고서가 표시된 Internet Explorer의 **파일>다른 이름으로 저장**을 선택합니다. <웹 페이지 저장>이 나타나면 파일을 저장한 위치와 파일 이름을 설정합니다.

❖ 인쇄: 사이트 분석 보고서가 표시된 Internet Explorer의 **파일>인쇄**를 선택합니다.

17장
안전도

안전한 프로그램 사용도

안전한 프로그램 사용도는 최근 7일간 사용자 PC에서 실행된 프로그램들을 분석하여 정상, 악성, 미확정으로 구분하여 안전도를 평가하는 기준입니다. 안전한 프로그램 사용도는 최근 7일간 사용자 PC에서 실행된 프로그램과 미확정으로 분류된 프로그램 사용 여부를 바탕으로 산정한 점수입니다.

안전한 프로그램 사용도는 0점~100점 사이의 점수로 표시하며 정상이 아니거나 미확정 프로그램을 실행할 때 마다 100점 만점을 기준으로 점수를 차감하여 계산합니다.

따라서, 사용자 PC의 안전한 프로그램 사용도에 대한 점수는 현재 PC 사용에 대한 안전도를 구분하는 척도로 활용할 수 있습니다.

- ❖ 안전: 안전도 점수가 100~80점 사이인 경우입니다.
- ❖ 주의: 안전도 점수가 79~60점 사이인 경우입니다.
- ❖ 위험: 안전도 점수가 60점 미만인 경우입니다.

참고

안전도 점수가 낮은 경우에는 미확정이나 악성으로 분류된 파일에 대해 클라우드 자동 분석을 요청하고 최신 엔진으로 업데이트하여 PC 검사를 실행할 것을 권장합니다.

안전한 사이트 사용도

안전한 사이트 사용도는 최근 7일간 사용자가 접속한 사이트들을 분석하여 정상, 악성, 미확정으로 구분하여 안전도를 평가하는 기준입니다. 안전한 사이트 사용도는 최근 7일간 사용자가 접속한 사이트와 미확정으로 분류된 사이트 접속 여부를 바탕으로 산정한 점수입니다.

안전한 사이트 사용도는 0점~100점 사이의 점수로 표시하며 정상이 아니거나 미확정 사이트에 접속할 때 마다 100점 만점을 기준으로 점수를 차감하여 계산합니다.

따라서, 사용자 PC의 안전한 사이트 사용도에 대한 점수는 현재 PC 사용에 대한 안전도를 구분하는 척도로 활용할 수 있습니다.

- ❖ 안전: 안전도 점수가 100~80점 사이인 경우입니다.
- ❖ 주의: 안전도 점수가 79~60점 사이인 경우입니다.
- ❖ 위험: 안전도 점수가 60점 미만인 경우입니다.

참고

안전도 점수가 낮은 경우에는 미확정이나 악성으로 분류된 파일에 대해 클라우드 자동 분석을 요청하고 최신 엔진으로 업데이트하여 PC 검사를 실행할 것을 권장합니다.


AhnLab

18장
환경 설정

실행 방법

환경 설정은 V3에서 사용할 수 있는 다양한 옵션에 대해 사용자가 직접 선택하여 사용할 수 있는 기능입니다.

바탕 화면에서 실행하기

1 바탕 화면의 V3 아이콘( )을 더블 클릭합니다.

2 V3가 실행되면 화면 오른쪽 위에 있는 환경 설정 아이콘( )을 선택합니다.

3 환경 설정이 나타나면, 각 항목별로 선택하여 V3 실행 환경을 설정합니다.

- PC 검사 설정
- 고급 설정
- 검사 예외 설정
- 네트워크 보안
- Active Defense
- 기타 설정

작업 표시줄에서 실행하기

❖ 작업 표시줄의 V3 아이콘( )에서 마우스 오른쪽을 눌러 환경 설정을 실행할 수 있습니다.

환경 설정의 공통 버튼

환경 설정의 각 화면에서 제공하는 버튼은 모두 기본값, 기본값, 확인, 취소가 있습니다. 각각의 버튼은 다음과 같이 작동합니다.

- ❖ 모두 기본값: 환경 설정의 모든 옵션을 V3에서 권장하는 기본값으로 변경합니다. 모두 기본값을 누르면, 사용자가 설정한 개별 옵션 값은 모두 지워지고 V3에서 설정한 기본값으로 모두 변경 적용됩니다.
- ❖ 기본값: V3에서 권장하는 기본 설정 값입니다. 기본값을 누르면, 선택한 화면에서 사용자가 설정한 개별 옵션 값은 모두 지워지고 V3에서 설정한 기본값으로 변경 적용됩니다.
- ❖ 확인: 설정한 내용을 저장하고 현재 창을 닫습니다.
- ❖ 취소: 설정한 내용을 저장하지 않고 현재 창을 닫습니다.

PC 검사 설정

PC 실시간 검사

PC 실시간 검사는 알려지거나 알려지지 않은 악성코드를 지속적으로 탐지하여 차단합니다. V3 사용자는 PC 실시간 검사 실행 전 검사할 사전 검사 대상과 PC 실시간 검사가 검사할 검사 대상과 치료 방법을 직접 설정하여 사용자에게 맞는 검사를 사용할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **PC 검사 설정>PC 실시간 검사** 탭을 선택합니다.

PC 실시간 검사에서 설정할 수 있는 옵션

❖ PC 실시간 검사 사용: PC 실시간 검사 사용 여부를 선택합니다. PC 실시간 검사를 사용하려면 이 옵션을 선택해야 합니다. PC 실시간 검사를 선택하면 PC 실시간 검사가 항상 작동하여 사용자 PC에서 발생하는 파일의 저장, 이동, 실행, 삭제, 네트워크 접근 등의 일련의 행위를 탐지하여 감염된 악성코드가 있는 경우 치료 방법에 따라 처리합니다.

- PC 실시간 검사 종료 후 자동으로 다시 시작: PC 실시간 검사를 종료했을 경우 자동으로 다시 시작할 시간을 설정합니다. 자동으로 다시 시작할 주기는 **10분 후, 30분 후, 60분 후, PC 다시 시작할 때**를 선택할 수 있으며, 선택한 시간이 지난 후에 PC 실시간 검사를 다시 시작합니다. **사용 안 함**을 선택하면, PC 실시간 검사를 종료한 후 자동으로 다시 시작하지 않습니다.

⚠ 주의

PC 실시간 검사를 사용하지 않으면, 실시간 검사가 작동하지 않아 악성코드의 위험에 노출될 위험이 높아집니다. 악성코드로 부터 PC를 안전하게 보호하기 위해 PC 실시간 검사를 항상 사용하고 PC 실시간 검사 종료 후 자동으로 다시 시작 옵션을 선택하거나 다시 시작 주기를 짧게 설정할 것을 권장합니다.

- 행위 기반 진단 사용: 다양하고 입체적인 방법으로 악성코드를 사전 대응하는 기술로 파일이 실행될 때 작동하는 행위에 대한 일련의 의심 행위 세트를 기반으로 악성코드를 진단합니다.
- 클라우드 평판 기반 실행 차단 사용: 안랩 클라우드 서버의 평판 정보를 기반으로 하여 평판 점수가 낮은 프로그램의 실행을 차단합니다. 평판 점수는 최초 발견 날짜, 사용자 수, 의심 행위 수에 대한 정보를 종합적으로 수집하여 계산합니다.
- 차단 수준: 평판 기반 실행 차단의 기준이 되는 차단 수준을 설정합니다. 차단 수준은 낮음, 보통(권장), 높음을 선택할 수 있습니다.
  - 낮음: 최초 발견 10일 이내, 사용자 수 100명 이하, 의심 행위 3건 이상인 파일에 대해 차단합니다.
  - 보통(권장): 최초 발견 20일 이내, 사용자 수 500명 이하, 의심 행위 1건 이상인 파일에 대해 차단합니다.
  - 높음: 최초 발견 30일 이내, 사용자 수 800명 이하, 의심 행위 0건 이상인 파일에 대해 차단합니다.

참고

행위 기반 진단, 클라우드 평판 기반 실행 차단은 PC 실시간 검사 사용을 선택한 경우에만 작동합니다.

사전 검사

PC 실시간 검사를 실행하기 전 검사할 대상을 설정합니다. 사전 검사 대상을 설정하려면, 사전 검사 사용을 먼저 선택해야 합니다.

❖ 사전 검사 사용: 사전 검사 대상을 설정하려면, 사전 검사 사용을 먼저 선택해야 합니다.

❖ 설정: 설정을 누르면 사전 검사 대상을 설정할 수 있습니다.

검사 대상

PC 실시간 검사에서 검사할 검사 대상 파일과 프로그램을 설정합니다.

❖ 설정: 설정을 누르면 검사 대상을 설정할 수 있습니다.

치료 방법

PC 실시간 검사에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

❖ 설정: 설정을 누르면 치료 방법을 설정할 수 있습니다.

정밀 검사

정밀 검사는 사용자가 검사 대상을 직접 선택하여 PC를 검사할 수 있는 기능입니다. 정밀 검사는 사용자가 선택한 검사 대상을 검사하므로 실시간 검사와 달리 V3 설치 이전의 감염된 파일을 검사할 수 있는 장점이 있지만, 선택한 파일의 개수와 종류에 따라 검사 시의 PC의 속도가 달라질 수도 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **PC 검사 설정>정밀 검사** 탭을 선택합니다.

검사 대상

정밀 검사에서 검사할 검사 대상 파일과 프로그램을 설정합니다.

❖ 설정: 설정을 누르면 검사 대상을 설정할 수 있습니다.

치료 방법

정밀 검사에서 발견한 감염된 대상을 치료하는 방법을 설정합니다.

❖ 설정: 설정을 누르면 치료 방법을 설정할 수 있습니다.

검사 옵션

정밀 검사시 설정할 수 있는 검사 옵션입니다.

❖ 공유 폴더 해제 후 검사: 정밀 검사를 실행할 때 사용자 PC에 공유 폴더가 있는 경우 공유를 해제하고 검사합니다. 공유 폴더 해제 후 검사를 실행하면, 검사 완료 후 공유 폴더를 다시 설정해 주지 않습니다.

예약 검사

예약 검사는 사용자가 설정한 날짜와 시간에 PC를 검사하는 기능입니다. 악성코드로 부터 PC를 안전하게 보호하려면 PC 실시간 검사 사용과 더불어 예약 검사를 주기적으로 사용하는 것이 좋습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **PC 검사 설정>예약 검사** 탭을 선택합니다.

예약 검사 목록

❖ 예약 검사 사용: 예약 검사 사용 여부를 선택합니다. 예약 검사 사용을 선택하면, 추가를 눌러 예약 검사 주기와 검사 대상과 치료 방법 등을 설정할 수 있습니다.

❖ 추가: 예약 검사 설정에서 검사 시간과 검사 영역, 검사 대상, 치료 방법 등을 설정할 수 있습니다. 추가한 예약 검사는 예약 검사 목록 화면에 표시됩니다.

❖ 수정: 예약 검사 목록에 추가한 예약 항목을 선택하여 검사 내용을 수정합니다.

❖ 삭제: 예약 검사 목록에 추가한 예약 항목을 선택하여 삭제합니다.

❖ 검사 이름: 예약 검사 설정에서 입력한 검사 이름을 표시합니다.

❖ 검사 시간: 예약 검사 설정에서 선택한 검사 시간을 표시합니다.

❖ 검사 영역: 예약 검사 설정에서 선택한 검사 영역을 표시합니다.

참고

예약 검사는 최대 10개까지 등록할 수 있으며 예약 검사 내용이 동일한 중복 예약 검사는 목록에 등록되지 않습니다.

예약 검사 추가

예약 검사 목록 화면에서 **추가**를 누르면 예약 검사를 추가할 수 있습니다.

❖ 검사 이름: 예약 검사를 구분할 수 있는 이름을 입력합니다.

❖ 검사 시간: 예약 검사를 실행할 시간을 선택합니다.

- 매일: 매일을 선택하면 검사 시간을 선택할 수 있습니다.

- 매주: 매주를 선택하면 요일과 검사 시간을 선택할 수 있습니다.
- 매월: 매월을 선택하면 특정 날짜와 검사 시간을 선택할 수 있습니다.
- 한 번만: 한 번만을 선택하면 검사할 날짜와 검사 시간을 선택할 수 있습니다.

❖ 검사 영역: 예약 검사에서 검사할 영역을 선택할 수 있습니다.

- 메모리/프로세스: 메모리에 실행 중인 프로그램과 프로세스를 검사합니다.
- 부트 레코드: C 드라이브의 부트 레코드와 부팅한 드라이브의 부트 영역의 감염 여부를 검사합니다.
- 중요 시스템 파일: 시작 프로그램 폴더, 바탕 화면 폴더, Windows 설치 폴더와 같은 V3가 선정한 중요 시스템 파일에 대해 검사합니다.
- 내 컴퓨터(로컬 디스크): 사용자 PC의 로컬 디스크(C 드라이브, D 드라이브 등)를 검사합니다.

❖ 검사 대상 설정: 설정을 누르면 검사 대상을 설정할 수 있습니다.

❖ 치료 방법 설정: 설정을 누르면 치료 방법을 설정할 수 있습니다.

사전 검사 대상 설정

사전 검사는 PC 실시간 검사 실행시 시스템의 중요한 영역을 먼저 검사하여 악성코드 감염 여부를 판별합니다. 사전 검사 사용 여부는 사용자가 직접 선택할 수 있으며, 사전 검사 영역에 감염된 악성코드는 모두 자동 치료합니다.

실행 방법

사전 검사 대상 설정은 PC 실시간 검사에서 설정할 수 있습니다.

사전 검사 대상 설정

❖ 부트 레코드: Windows가 설치된 드라이브의 부트 레코드를 검사합니다. 일반적으로 Windows는 C 드라이브에 설치하므로 대부분은 C 드라이브의 부트 레코드를 검사합니다. Windows를 C 드라이브가 아닌 D 드라이브 같은 다른 드라이브에 설치했다면 부팅한 드라이브의 부트 레코드를 검사합니다.

❖ 메모리/프로세스: PC의 메모리에 실행 중인 프로그램과 현재 실행 중인 프로세스를 검사합니다. 악성코드가 실행되면, 대부분 메모리와 프로세스에 로드되어 다른 프로그램을 감염시키는 경우가 많습니다.

참고

프로그램은 디스크에 저장된 파일이고, 프로세스는 메모리에서 실행 중인 복사된 프로그램입니다. 따라서,악성코드가 실행되면 악성코드가 실행한 프로세스가 실행 중일 가능성이 높습니다. 현재 실행 중인 프로세스는 Windows의 작업 관리자를 실행(Ctrl+Alt+DEL키를 누름)하여 [프로세스]에서 확인할 수 있습니다.

검사 대상 설정

검사 대상은 V3의 PC 검사에서 검사할 파일이나 프로그램을 선택하는 기능입니다. 검사 대상은 PC 실시간 검사, 정밀 검사, 예약 검사에서 각각 설정할 수 있으며 검사 종류별로 선택할 수 있는 검사 대상에는 차이가 있습니다.

실행 방법

검사 대상 설정은 PC 실시간 검사, 정밀 검사, 예약 검사에서 설정할 수 있습니다.

PC 실시간 검사의 검사 대상 설정

- ❖ 불필요한 프로그램: 사용자 동의를 받고 설치했지만, 사용자가 알고 있는 프로그램의 설치 목적과 관계가 없는 행위를 하는 것으로 알려진 잠재적 위험이 있는 프로그램을 불필요한 프로그램으로 판단하여 검사합니다.
- ❖ 평판이 낮은 프로그램: ASD 클라우드 서버의 평판 정보를 이용하여 악성과 정상 여부가 검증되지 않은 파일에 대해 검사합니다. 평판 점수는 최초 발견 날짜, 사용자 수, 의심 행위, 해당 프로그램에 대한 신뢰나 차단 횟수를 종합하여 판단합니다.
- ❖ 네트워크 드라이브: 사용자가 네트워크 드라이브에 있는 파일을 실행할 때 감염 여부를 검사하여 해당 파일이 감염되었을 경우 알려줍니다.

정밀 검사/예약 검사의 검사 대상 설정

- ❖ 유해 가능 프로그램: 키로거나 원격 접속 툴 등 V3에서 유해 가능 프로그램으로 분류한 파일에 대해 검사합니다.
- ❖ 불필요한 프로그램: 사용자 동의를 받고 설치했지만, 사용자가 알고 있는 프로그램의 설치 목적과 관계가 없는 행위를 하는 것으로 알려진 잠재적 위험이 있는 프로그램을 불필요한 프로그램으로 판단하여 검사합니다.

❖ 평판이 낮은 프로그램: ASD 클라우드 서버의 평판 정보를 이용하여 악성과 정상 여부가 검증되지 않은 파일에 대해 검사합니다. 평판 점수는 최초 발견 날짜, 사용자 수, 의심 행위, 해당 프로그램에 대한 신뢰나 차단 횟수를 종합하여 판단합니다.

❖ EML 파일: EML 파일의 본문과 첨부 파일을 검사합니다. 감염된 첨부 파일은 사용자가 선택한 치료 방법에 따라 치료하고 다시 첨부합니다. 단, EML 파일에 다시 첨부된 EML 파일이 있는 다중 EML 파일인 경우에는 검사하지 않습니다.

❖ 압축 파일: 압축된 파일을 검사합니다. 압축 파일을 검사 대상으로 선택하면, 압축 횟수를 선택하여 검사할 수 있습니다.

- 검사할 최대 다중 압축 횟수(1~5회): 사용자가 설정한 최대 다중 압축 횟수에 따라 압축을 풀어 검사합니다. 다중 압축 횟수는 1부터 5까지 설정할 수 있습니다. 다중 압축 횟수가 높은 파일을 검사할 경우 검사 시간이 오래 걸릴 수 있습니다. 기본 값은 1(회)입니다.

치료 방법 설정

치료 방법 설정은 악성코드에 감염된 대상을 치료하는 방법을 선택하는 기능입니다. 치료 방법은 감염된 대상과 감염 상태에 따라 자동 치료하거나 삭제, 치료 안 함 등을 선택할 수 있으며 감염된 파일을 검역소에 보관할 수도 있습니다.

실행 방법

치료 방법 설정은 PC 실시간 검사, 정밀 검사, 예약 검사에서 설정할 수 있습니다.

PC 실시간 검사의 치료 방법 설정

❖ 악성코드 감염 파일: 악성코드에 감염된 파일에 대한 치료 방법을 설정합니다.

- 치료: 감염된 파일을 치료합니다.
- 치료 안 함: 감염된 파일을 치료하지 않고 감염 상태 그대로 둡니다.

❖ 치료/삭제 전 검역소로 보내기: 감염된 파일을 치료하거나 삭제하기 전에 감염된 상태 그대로 검역소에 보관합니다.

정밀 검사/예약 검사의 치료 방법 설정

❖ 감염된 압축 파일: 압축 파일이 감염되어 있을 경우 치료 방법을 설정합니다.

- 치료 안 함: 감염된 압축 파일을 치료하지 않고 감염 상태 그대로 둡니다.
- 삭제: 감염된 압축 파일을 삭제합니다.

❖ 자동 치료: 악성코드에 감염된 파일을 자동 치료합니다. 자동 치료를 선택하면, 악성코드 발견시 치료 방법을 사용자에게 확인하지 않고 치료합니다.

❖ 치료/삭제 전 검역소로 보내기: 감염된 파일을 치료하거나 삭제하기 전에 감염된 상태 그대로 검역소에 보관합니다.

참고

자동 치료는 정밀 검사에서만 선택할 수 있으며, 예약 검사의 치료 방법에서는 자동 치료를 지원하지 않습니다.

고급 설정

고급 검사

고급 검사에서는 PC 검사에서 사용할 수 있는 기본적인 검사 옵션외의 다양한 검사 옵션을 사용자가 직접 선택할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **고급 설정>고급 검사** 탭을 선택합니다.

고급 검사에서 설정할 수 있는 옵션

❖ CD/USB 드라이브 자동 실행 방지: USB 메모리를 연결했을 때 이동식 디스크의 내용을 보여주는 창이 실행되지 않아 폴더 구조를 보이지 않게 하고 CD를 꽂았을 때 자동 실행되지 않게 합니다. 자동 실행(AutoRun) 기능을 이용하여 감염되는 악성코드로 부터 사용자 PC를 보호하려면 CD나 USB 메모리에 저장된 파일을 자동 실행하지 않고 사용자가 직접 실행하여 감염된 파일의 자동 실행(AutoRun)으로 인해 PC가 감염되는 것을 예방할 수 있습니다.

❖ USB 드라이브 자동 검사: USB 드라이브에 저장 매체가 연결되었을 경우 자동 검사합니다.

- 모든 하위 폴더 검사: USB 드라이브에 저장된 하위 폴더를 모두 검사합니다.
- 검사 창 띄우지 않기: USB 드라이브 자동 검사를 할 때 검사 창을 화면에 표시하지 않습니다.

❖ 스마트 검사: 스마트 검사는 Windows가 설치한 파일에 대해서는 안전하다고 판단하여 검사를 생략하고, 이전의 검사에서 검사 후 변경되지 않은 검사 대상에 대해서는 검사를 생략하는 검사 방법입니다. 스마트 검사를 사용하면 검사 속도를 높이는데 도움이 됩니다.

❖ V3 무결성 정기 검사: PC를 시작할 때 V3 파일의 무결성을 검사합니다. 무결성 검사는 V3 파일에 대한 디지털 서명을 바탕으로 변경 여부를 확인합니다.

❖ V3 감염 여부 검사: V3 프로그램의 악성코드 감염 여부를 검사합니다. V3가 악성코드에 감염된 경우에는 프로그램을 종료하여 감염된 파일을 치료한 후 다시 프로그램을 시작합니다.

❖ V3 제품 보호: V3 이외의 다른 프로그램에서 V3가 사용하는 프로세스, 레지스트리, 파일, V3 설치 볼륨에 접근하는 것을 차단합니다. 설정을 누르면 V3 제품 보호 대상 설정에서 보호 대상을 선택할 수 있습니다.

- V3 제품 보호 종료 후 자동으로 다시 시작: V3 제품 보호를 종료했을 경우 자동으로 다시 시작할 시간을 설정합니다. 자동으로 다시 시작할 주기는 **10분 후, 30분 후, 60분 후, PC 다시 시작할 때**를 선택할 수 있으며, 선택한 시간이 지난 후에 V3 제품 보호를 다시 시작합니다. **사용 안 함**을 선택하면, V3 제품 보호를 종료한 후 자동으로 다시 시작하지 않습니다.

❖ 중요 시스템 파일 보호: 시스템 보호를 위해 마스터 부트 레코드나 중요 시스템 파일과 같은 시스템 보호 대상에 대한 접근을 차단합니다.

❖ TrueFind(은폐형 악성코드 진단) 사용: TrueFind는 악성코드가 자신의 정보를 발견할 수 없도록 숨겼을 때 은폐된 악성코드를 탐지하는 기능입니다. V3에서 은폐형 악성코드를 발견하면 부트 타임 검사를 이용해 치료합니다.

시스템 복원 지점 생성

시스템 복원 지점 생성은 PC에 문제가 발생했을 경우에 대비하여 특정 시점의 PC 상태를 백업하여 두는 기능입니다.

❖ 시스템 복원 지점 생성 사용: 시스템 복원 지점 생성을 사용하면, Windows에 프로그램을 설치할 때, 패치나 업데이트 설치, PC 검사에서 악성코드를 치료할 때, PC 최적화를 실행하기 전 상태에 대해 백업합니다.

참고

Windows 8에서는 운영 체제의 특성상 하루 1번만 복원 지점 생성이 허용됩니다. 또한, 안전 모드로 부팅했을 경우에는 시스템 복원 지점 생성 사용을 선택했더라도 복원 지점이 생성되지 않습니다.

V3 제품 보호 대상 설정

V3 제품 보호를 선택하고 **설정**을 누르면 V3 제품 보호 대상을 설정할 수 있습니다. V3 제품 보호 대상은 프로세스, 레지스트리, 파일, 볼륨이 있습니다.

- ❖ 프로세스: V3 이외의 다른 프로그램이 V3 프로세스를 종료하는 것을 차단합니다.
- ❖ 레지스트리: V3 이외의 다른 프로그램이 V3 관련 레지스트리를 변경하거나 삭제 시도하는 것을 차단합니다.
- ❖ 파일: V3 이외의 다른 프로그램이 V3 관련 파일을 변경하거나 삭제 시도하는 것을 차단합니다.
- ❖ 볼륨: V3 이외의 다른 프로그램이 V3 설치 볼륨을 변경하거나 삭제 시도하는 것을 차단합니다.

클라우드

안랩의 ASD(AhnLab Smart Defense) 클라우드 서버의 악성코드 데이터베이스를 활용하여 파일의 악성 여부를 검사하고 클라우드 서버에 보고되지 않은 새로운 파일을 발견했을 때는 해당 파일을 서버로 전송하여 실시간으로 분석하고 결과를 사용자에게 알려줍니다. 클라우드 서비스를 활용하면, 알려지지 않은 위협에 빠르게 대처할 수 있어 악성코드 감염으로 인한 위협을 감소시키는데 도움이 됩니다.

실행 방법

1. V3 실행 후 환경 설정을 선택합니다.
2. **고급 설정>클라우드** 탭을 선택합니다.

클라우드 진단 설정

V3 엔진을 통한 악성코드 검사와 더불어 클라우드 서버의 데이터베이스의 정보를 기반으로한 클라우드 진단의 진단 수준을 설정합니다.

- ❖ 진단 수준: 클라우드 진단에서 악성코드로 판단할 수준을 설정합니다.
  - 낮음: 의심 파일이 악성코드일 가능성이 매우 큰 위험 요소만 차단합니다.
  - 보통(권장): 의심 파일이 악성코드일 가능성이 일정 기준 이상이 되는 경우에 차단합니다.
  - 높음: 악성코드로 추측되는 모든 경우를 차단하지만, 오진의 가능성이 있을 수 있습니다.

검사 예외 설정

검사 예외 설정

검사 예외 설정은 PC 검사의 검사 대상에 포함되더라도 사용자가 설정한 검사 예외 대상이거나 악성코드이지만 사용자가 검사 예외 악성코드로 설정한 경우에는 설정된 대상과 항목에 대해서는 검사하지 않는 기능입니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **검사 예외 설정**을 선택합니다.

검사 예외 사용

검사 예외 대상이나 검사 예외 악성코드를 설정하려면 검사 예외 사용을 선택해야 합니다.

> **참고**
> 검사 예외 사용을 선택하지 않으면, 검사 예외 대상이나 검사 예외 악성코드를 설정할 수 없습니다.

검사 예외 대상 설정

검사하지 않을 폴더나 파일을 추가하는 기능입니다.

> **주의**
> 검사 예외로 추가한 대상은 악성코드에 감염된 경우에도 검사하지 않으므로 반드시 필요한 경우에만 사용하십시오.

검사 예외 폴더 추가

검사하지 않을 폴더를 추가합니다. 검사 예외 폴더 추가는 검사 예외 대상 설정에서 **폴더 추가**를 눌러 설정할 수 있습니다.

❖ 폴더 추가: 검사 예외 대상에서 **폴더 추가**를 누르면 나타나는 <폴더 찾아보기> 에서 추가할 폴더를 선택하고 **확인**을 누릅니다. 선택한 폴더가 검사 예외 목록의 검사 예외 대상으로 등록되었는지 확인합니다.

검사 예외 파일 추가

검사하지 않을 파일을 추가합니다. 검사 예외 파일 추가는 검사 예외 대상 설정에서 **파일 추가**를 눌러 설정할 수 있습니다.

❖ 파일 추가: 검사 예외 대상에서 **파일 추가**를 누르면 나타나는 <열기>에서 추가할 파일을 선택하고 **확인**을 누릅니다. 선택한 파일이 검사 예외 목록의 검사 예외 대상으로 등록되었는지 확인합니다.

검사 예외 목록 삭제

검사 예외 목록에 추가된 폴더나 파일을 삭제하여 검사 예외 대상에서 제외합니다. 검사 예외 목록 삭제는 검사 예외 대상 목록에서 삭제 대상을 선택하고 **삭제**를 눌러 설정할 수 있습니다.

❖ 삭제: 검사 예외 대상에서 삭제 대상을 선택하고 **삭제**를 누릅니다. **선택한 검사 예외 목록을 삭제하시겠습니까?** 라는 메시지가 나타나면 **예**를 누릅니다. 선택한 대상이 검사 예외 대상 목록에서 삭제되었는지 확인합니다.

검사 예외 악성코드 설정

검사하지 않을 악성코드를 추가하는 기능입니다.

> ⚠ **주의**
> 검사 예외로 추가한 악성코드는 악성코드로 알려져 있지만, 검사에서 제외하므로 반드시 필요한 경우에만 사용하십시오.

검사 예외 악성코드 추가

검사에서 제외할 악성코드를 추가합니다. 검사 예외 악성코드 설정에서 **추가**를 누르면, 검사 예외 악성코드로 추가할 수 있습니다.

❖ 추가: 검사 예외 악성코드 설정에서 **추가**를 누르면 나타나는 <검사 예외 악성코드 추가/수정>에 악성코드 이름을 입력합니다. 악성코드 이름은 V3에서 진단한 이름과 동일하게 입력해야 합니다. 악성코드 이름을 입력하고 **확인**을 누르고, 입력한 악성코드 이름이 목록에 등록되었는지 확인합니다.

검사 예외 악성코드 수정/삭제

검사 예외 악성코드 목록에 등록된 악성코드 이름을 수정하거나 목록에서 삭제합니다. 검사 예외 악성코드 목록에서 수정/삭제할 대상을 선택하고 수정/삭제를 누르면 대상을 수정하거나 삭제할 수 있습니다.

- ❖ 수정: 검사 예외 악성코드 목록에서 대상을 선택하고 **수정**을 누르면 나타나는 <검사 예외 악성코드 추가/수정>에서 악성코드 이름을 수정합니다. **확인**을 누른 후 수정한 악성코드 이름이 목록에 등록되었는지 확인합니다.
- ❖ 삭제: 검사 예외 악성코드 목록에서 대상을 선택하고 **삭제**를 누릅니다. **선택한 검사 예외 대상을 삭제하시겠습니까?** 라는 메시지가 나타나면 **예**를 누릅니다. 선택한 검사 예외 악성코드가 목록에서 삭제되었는지 확인합니다.

시스템 복원 폴더 검사 설정

시스템 복원 폴더는 Windows가 시스템 복원을 위해 PC를 손상시킬 수 있는 변경 내용을 추적할 수 있도록 제공하는 기능입니다. 시스템 복원 폴더는 Windows만 해당 폴더를 생성하고 파일을 저장할 수 있기 때문에 복원 폴더에서 발견된 감염 파일은 백신 프로그램이 쓰기 권한이 없으므로 치료할 수 없습니다.

시스템 복원 폴더에서 악성코드가 발견되는 이유는 Windows가 시스템 복원 폴더에 파일을 백업할 때 이미 감염된 파일을 백업했기 때문입니다. 따라서, 시스템 복원 폴더에서 악성코드가 발견되었을 경우에는 치료할 수는 없습니다.

시스템 복원 폴더에 저장된 파일로 시스템을 복원할 때 감염된 파일로 복원을 하면 PC가 감염된 상태로 복원이 됩니다. 따라서, 시스템 복원을 할 때 해당 파일이 악성코드에 감염되었음을 사용자가 알고 있는 것이 중요합니다.

Windows XP와 Windows 7의 경우 시스템 복원 폴더는 Windows 설치 드라이브:\WINDOWS\system32\Restore 입니다.

- ❖ 시스템 복원 폴더 검사 안 함: 시스템 복원 폴더를 검사하지 않습니다.

참고

Windows 2000에서는 시스템 복원 폴더 검사 안 함을 사용할 수 없습니다.

네트워크 보안

웹 보안

웹 보안은 피싱 사이트나 악성 파일을 다운로드하게 하는 악성 사이트, 사용자가 지정한 차단 사이트에 대한 접근을 차단하는 기능입니다.

차단 대상 사이트에 접속하면 접속을 차단하고 사이트 차단 페이지가 나타납니다. 성인 사이트나 도박 사이트와 같은 유해한 사이트를 등록하거나 회사나 단체에서 접속이 금지된 사이트를 등록하면 유해 사이트 접속으로 인한 문제를 예방할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **네트워크 보안>웹 보안**을 선택합니다.

유해 사이트 차단 사용

❖ 유해 사이트 차단: 웹 보안에서 제공하는 사이트 차단 기능을 사용하려면 유해 사이트 차단을 선택해야 합니다. 유해 사이트는 홈페이지 변조를 통해 사용자들이 해당 사이트에 접속했을 때 악성코드를 다운로드하게 하는 유형의 사이트를 말하며 안랩 ASD 클라우드 서버에 수집된 사이트 주소를 기준으로 판단합니다.

- 피싱 사이트 차단: 피싱 사이트는 사용자를 속이는 사기성 사이트로 Anti-Phishing Working Group의 데이터베이스를 바탕으로 판단합니다. 피싱 사이트를 차단하려면 유해 사이트 차단을 선택해야 합니다.
- 불필요한 사이트(PUS) 차단: 불필요한 사이트(PUS: Potentially Unwanted Site)는 악성코드를 유포하거나 피싱 사이트에는 해당하지 않지만 불필요한 프로그램(PUP)의 설치를 유도하거나 사용자에게 불필요한 사이트로 유도하는 사이트를 의미합니다. 불필요한 사이트 차단을 선택하면 이러한 행위를 하는 것으로 알려진 사이트에 대한 접속을 차단합니다. 불필요한 사이트를 차단하려면 유해 사이트 차단을 선택해야 합니다.

사용자 지정 사이트 관리

사용자 지정 사이트 관리는 V3 사용자가 신뢰하거나 접속을 차단할 사이트 목록을 추가할 수 있는 기능입니다. 사용자 지정 사이트 관리를 사용하려면 유해 사이트 차단을 선택해야 합니다.

- ❖ 주소: 신뢰 또는 차단할 사이트의 주소를 입력합니다.
- ❖ 신뢰 추가: 주소에 입력한 사이트를 신뢰 사이트로 등록합니다. 신뢰 추가를 누르면 입력한 사이트의 상태 값이 신뢰로 등록되어 사용자 지정 사이트 목록에 표시됩니다.
- ❖ 차단 추가: 주소에 입력한 사이트를 차단 사이트로 등록합니다. 차단 추가를 누르면 입력한 사이트의 상태 값이 차단으로 등록되어 사용자 지정 사이트 목록에 표시됩니다.
- ❖ 삭제: 사용자 지정 사이트 관리 목록에 등록된 사이트를 목록에서 삭제합니다. 삭제를 누르면, **선택한 사이트 주소를 목록에서 삭제하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 선택한 사이트를 목록에서 삭제합니다.

참고

사용자 지정 사이트 관리 목록에는 최대 300개까지 추가할 수 있습니다.

네트워크 침입 차단

최근의 악성코드는 네트워크를 통해 침입하여 순식간에 확산되는 특징을 가지고 있습니다.

네트워크 침입 차단은 네트워크를 통해 웜이나 트로이목마와 같은 악성코드가 침입하는 것을 탐지하여 차단합니다. 악성코드에 감염된 PC는 네트워크로 연결된 다른 PC를 감염시킵니다. 네트워크에 감염된 PC가 있으면 사용자의 PC도 악성코드에 감염될 위험이 있습니다. 특히 인터넷에 연결된 PC는 항상 악성코드에 감염될 위험이 있습니다.

네트워크 침입 차단을 사용하면 패킷의 특정 서명 정보를 기반으로 악성코드를 탐지하여 PC를 보호할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **네트워크 보안>침입 차단>네트워크 침입 차단** 탭을 선택합니다.

네트워크 침입 차단 사용 여부 선택

❖ 네트워크 침입 차단 사용: 네트워크 침입 차단 기능을 사용하도록 설정합니다. 네트워크 침입 차단을 사용하면 침입 차단 규칙에 따라 사용자 PC를 보호합니다.

참고

네트워크 침입 차단을 사용하지 않으면 웜이나 트로이목마와 같은 해킹 위험에 노출될 수 있습니다.

❖ 차단 규칙 보기: 네트워크 침입 차단 규칙 목록을 확인할 수 있습니다. 네트워크 침입 차단 규칙 목록에서는 규칙을 최적화하거나 규칙의 사용 여부를 사용자가 선택할 수 있습니다.

참고

네트워크 침입 차단에서 제공하는 차단 규칙은 엔진 업데이트에 의해 업데이트되므로 항상 최신 버전의 엔진을 사용할 것을 권장합니다.

IP 주소 허용/차단 설정

사용자가 설정한 IP 주소에 대해 네트워크 연결을 허용하거나 차단합니다.

❖ IP 주소 허용/차단 사용: 차단 IP 주소나 연결 IP 주소에 등록된 IP에 대하여 네트워크 연결을 차단하거나 허용합니다.

- 공격자 IP 임시 차단 사용: 네트워크 침입 차단 규칙에 의해 차단된 IP 주소에 대하여 해당 IP 주소에서 들어오는 모든 Inbound 트래픽을 30분간 차단합니다.

차단 IP 주소 추가

차단 IP 주소로 설정된 IP에서 들어오는 모든 Inbound 트래픽을 계속 차단합니다.

❖ 추가: <IP 주소 추가/수정>에서 차단할 IP 주소를 입력할 수 있습니다.

❖ 수정: 차단 IP 목록에서 수정할 IP 주소를 선택하고 수정을 누르면 <IP 주소 추가/수정>에서 IP 주소를 수정할 수 있습니다.

❖ 삭제: 차단 IP 목록에서 삭제할 IP 주소를 선택하고 삭제를 누르면 차단 IP 목록에서 지워집니다. 목록에서 삭제되면 더 이상 해당 IP 주소에서 들어오는 모든 Inbound 트래픽을 차단하지 않습니다.

❖ 연결 허용: 차단 IP 목록에 있는 IP 주소를 선택하고 연결 허용을 누르면, 연결 IP 주소로 해당 IP가 이동합니다.

❖ 계속 차단: 임시 차단 IP로 등록된 공격자 IP 주소를 계속 차단합니다. 공격자 IP 임시 차단 사용을 선택하면 차단 IP 주소에 등록하여 30분간 차단합니다. 30분이 지난 후에도 계속 차단하고 싶은 경우에 계속 차단을 선택하면, 등록된 공격자 IP 주소를 차단 IP 주소로 등록하여 차단합니다.

❖ IP 주소: 차단 IP 주소 목록에서 차단할 IP 주소를 보여줍니다.

❖ 차단 종료 시간: 등록된 IP 주소에 대한 차단 종료 시간을 보여줍니다.

허용 IP 주소 추가

허용 IP 주소로 등록된 IP 주소의 Inbound와 Outbound 트래픽에 대하여 네트워크 침입 차단 규칙이나 안랩 클라우드 서버의 악성 IP 조회를 적용하지 않고 모두 연결을 허용합니다.

❖ 추가: <IP 주소 추가/수정>에서 허용할 IP 주소를 입력할 수 있습니다.

❖ 수정: 허용 IP 목록에서 수정할 IP 주소를 선택하고 수정을 누르면 <IP 주소 추가/수정>에서 IP 주소를 수정할 수 있습니다.

❖ 삭제: 허용 IP 목록에서 삭제할 IP 주소를 선택하고 삭제를 누르면 허용 IP 목록에서 지워집니다. 목록에서 삭제되면 더 이상 해당 IP 주소에서 들어오는 모든 Inbound와 Outbound 트래픽의 연결을 항상 허용하지 않습니다.

❖ IP 주소: 허용 IP 주소 목록에서 허용할 IP 주소를 보여줍니다.

규칙 수정과 최적화

네트워크 침입 차단 규칙 목록에서는 규칙의 사용 여부를 사용자가 직접 선택할 수 있으며 필요없는 규칙을 사용하지 않도록 하는 규칙 최적화를 실행할 수 있습니다.

실행 방법

1 환경 설정>네트워크 보안>침입 차단에서 **네트워크 침입 차단 사용**을 선택합니다.

2 **차단 규칙 보기**를 누르면, <네트워크 침입 차단 규칙 목록>이 나타납니다.

네트워크 침입 차단 규칙 목록

❖ 규칙 이름: 네트워크 침입 차단 규칙의 이름을 보여줍니다. 각각의 규칙은 규칙에 정의된 패턴과 네트워크 트래픽을 비교하여 침입을 탐지하거나 차단합니다.

❖ 사용 여부: 규칙의 사용 여부나 최적화 완료 여부를 보여줍니다.

❖ 규칙 분류: 해당 규칙의 용도를 표시합니다. 규칙 분류는 취약점, 웜, 쉘코드, 악성코드, 해킹툴, 시스템으로 구분하여 표시합니다.

❖ 수정: 네트워크 침입 차단 규칙 목록에서 수정할 규칙을 선택하고 **수정**을 누르면, <네트워크 침입 차단 규칙 수정>에서 규칙의 사용 여부를 선택할 수 있습니다.

- 네트워크 침입 차단 규칙 수정: 규칙의 사용 여부 선택 및 규칙 이름과 규칙 분류를 확인할 수 있습니다.

참고

네트워크 침입 차단 규칙 목록에서 수정할 규칙을 선택하고 마우스 오른쪽을 누르면 나타나는 **사용/사용 안 함**을 눌러 규칙 사용 여부를 선택할 수도 있습니다.

❖ 규칙 최적화: 사용자 PC가 네트워크 규칙에 정의된 취약점에 대한 보안 패치가 이미 설치되어 있는 경우 해당 규칙을 자동으로 사용 안 함으로 변경합니다. 규칙 최적화를 사용하면, 네트워크 침입 차단 규칙 중 사용자 PC에 필요없는 규칙을 사용하지 않도록 설정하여 꼭 필요한 규칙만 작동하도록 합니다.

IP 주소 추가/수정

허용 IP 주소나 차단 IP 주소에 대상 IP를 등록하려면 IP 주소 추가/수정에서 IP 주소를 등록해야 합니다.

등록한 IP는 네트워크 침입 차단 규칙에 관계없이 항상 연결하거나 항상 차단합니다.

실행 방법

1 환경 설정>네트워크 보안>침입 차단에서 **네트워크 침입 차단 사용**을 선택합니다.

2 **IP 주소 허용/차단 사용**을 선택합니다.

3 차단 IP 주소나 허용 IP 주소에서 **추가**를 누르면 <IP 주소 추가/수정>이 나타납니다.

4 **입력 방법**에서 IP 주소 입력 방법을 선택하고 입력 방법에 따라 IP 주소를 입력합니다.

참고

IP 주소가 IPv4인 경우: 루프백 IP 주소인 127.0.0.1을 제외한 1.0.0.0~223.255.255.255 범위의 모든 주소를 입력할 수 있습니다.

IP 주소가 IPv6인 경우: 특정 용도로 이미 사용 중인 0:0:0:0:0:0:0:0, ::1, fe80::1, ::FFFF:0:0/96, fc00::/7, fd01::1f를 제외한 모든 주소를 입력할 수 있습니다.

IP 주소 입력 방법

❖ 단일 IP 주소/서브넷 마스크: 사용자가 입력한 특정 IP 주소나 서브넷 마스크를 연결하거나 차단합니다.

참고

IP 주소 입력 방법은 IP 주소/서브넷 마스크의 형식으로 입력해야 합니다.

IP 주소가 IPv4인 경우: 서브넷 마스크에 1~32까지 입력할 수 있습니다. 예) 192.168.0.12/1, 192.168.0.12/24, 192.168.0.12/32

IP 주소가 IPv6인 경우: 서브넷 마스크에 1~128까지 입력할 수 있습니다. 예) 2002:9b3d:1a32:4:208:74ff:fe39:0/112, 2002:9b3d:1a32:4:208:74ff:fe39:0/128

❖ IP 주소 범위: 시작 IP 주소와 종료 IP 주소 사이에 있는 IP 주소를 연결하거나 차단합니다.

- 시작 IP 주소: IP 주소 범위의 처음 IP 주소를 입력합니다.
- 종료 IP 주소: IP 주소 범위의 마지막 IP 주소를 입력합니다.

참고

종료 IP 주소는 시작 IP 주소 보다 커야 합니다.

행위 기반 침입 차단

행위 기반 침입 차단은 비정상적인 패킷의 흐름을 모니터링하여 이상 여부를 판단합니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **네트워크 보안>침입 차단>행위 기반 침입 차단** 탭을 선택합니다.

행위 기반 침입 차단 사용 여부 선택

❖ 행위 기반 침입 차단 사용: 행위 기반 침입 차단 기능을 사용하도록 설정합니다. 행위 기반 침입 차단을 사용하면 침입 차단 규칙에 따라 사용자 PC를 보호합니다.

처리 방법 선택

행위 기반 침입 차단에서 선택할 수 있는 각 항목의 처리 방법은 탐지, 차단, 사용 안 함 중에서 선택할 수 있습니다. 각 항목을 선택하면 다음과 같이 작동합니다.

❖ 탐지: 이상 패킷을 탐지하면 알림 창으로 알려줍니다. 사용자가 알림 창에서 차단 여부를 선택할 수 있습니다.

❖ 차단: 이상 패킷을 탐지하면 차단합니다.

❖ 사용 안 함: 이상 패킷을 탐지해도 알림 창으로 알려주거나 차단하지 않습니다.

알려지지 않은 프로토콜 드라이버

Outbound로 나가는 알려지지 않은 프로토콜 드라이버를 탐지하여 이상 패킷을 발견했을 경우 차단합니다.

❖ 파일 인증 정보 사용: 신뢰할 수 있는 디지털 인증서가 있는 경우에는 패킷을 차단하지 않습니다. 단, 최초 1회는 이상 패킷으로 간주하여 패킷을 차단할 수 있으나 인증서 확인 후에는 이상 패킷으로 차단하지 않습니다.

❖ 예외 목록: 알려지지 않은 프로토콜 드라이버 예외 목록을 추가할 수 있습니다. 예외 목록에 추가한 프로토콜이나 프로세스는 이상 패킷을 발생시키더라도 탐지하거나 차단하지 않습니다.

이상 트래픽

현재 프로세스에서 발생하는 Outbound 트래픽 중 기준치 이상의 패킷을 발송하는 경우에 DDos 공격으로 규정하여 탐지합니다. 이상 트래픽 탐지의 정확성을 높이기 위해 안랩에서 정한 규칙에 따라 일정 횟수 이상 지속적으로 발생하는 트래픽이 있는 경우 이상 트래픽으로 판단하여 처리합니다. 이상 트래픽의 대표적인 예로는 짧은 기간에 많이 발생하는 패킷, 비정상적으로 단편화된 패킷, 변칙적인 TCP 플래그가 지정된 패킷, 지나치게 잦은 HTTP 통신 패킷 등이 있습니다.

IP 스푸핑

IP 스푸핑은 공격자가 자신의 IP 주소를 변조하여 패킷을 내보내는 공격입니다. V3에서는 PC에서 발생하는 패킷의 출발지 IP 주소와 실제 IP 주소가 다른 패킷이 발송될 때 IP 스푸핑으로 판단하여 처리합니다.

참고

IP 주소는 네트워크 연결에서 해당 PC를 구분하는 고유 정보입니다. IP 스푸핑은 공격자가 자신의 IP 주소를 조작하는 네트워크 공격으로 공격자의 PC가 자신의 IP 주소가 아닌 다른 IP 주소로 위장하여 통신을 시도하는 공격 기법입니다. 공격 대상이 신뢰하는 IP 주소로 위장하여 접속하면 정보를 빼내거나 네트워크 공격을 시도할 수도 있습니다.

MAC 스푸핑

MAC 스푸핑은 공격자가 자신의 MAC 주소를 변조하여 패킷을 내보내는 공격입니다. V3에서는 PC에서 발생하는 패킷의 출발지 MAC 주소와 실제 MAC 주소가 다른 패킷이 발송될 때 MAC 스푸핑으로 판단하여 처리합니다.

참고

MAC 주소는 네트워크 연결에서 IP 주소와 함께 해당 PC를 구분하는 고유 정보입니다. MAC 스푸핑은 공격자가 자신의 MAC 주소를 조작하는 네트워크 공격으로 공격자의 PC가 자신의 MAC 주소가 아닌 다른 MAC 주소로 위장하여 통신을 시도하는 공격 기법입니다. 공격 대상이 신뢰하는 게이트웨이의 MAC 주소로 위장하여 접속하면 정보를 빼내거나 네트워크 공격을 시도할 수도 있습니다.

ARP 스푸핑

ARP 스푸핑은 공격자가 자신의 PC를 게이트웨이로 위장하여 패킷을 내보내는 공격입니다. V3에서는 실제 게이트웨이의 ARP 정보와 네트워크의 ARP 통신을 감시하여 PC가 게이트웨이인 것처럼 위장하여 보낸 ARP 통신을 ARP 스푸핑으로 판단하여 처리합니다.

참고

ARP(Address Resolution Protocol)는 네트워크 프로토콜의 일종으로 주소 결정 프로토콜을 의미합니다. ARP 스푸핑은 해커가 자신의 PC를 게이트웨이인것처럼 위장하기 위해 ARP를 조작하여 공격을 시도하는 해킹 유형입니다.

❖ 예외 목록: ARP 스푸핑 예외 목록을 추가할 수 있습니다. 예외 목록에 추가한 게이트웨이, IP 주소, MAC 에서 이상 패킷을 발생시키더라도 탐지하거나 차단하지 않습니다.

예외 목록

예외 목록은 행위 기반 침입 차단에서 설정한 항목을 탐지하거나 차단하도록 선택했을 때 탐지나 차단 규칙을 적용하지 않을 대상을 설정하는 기능입니다. 예외 목록에 추가한 대상에서 이상 트래픽을 발생시키더라도 탐지하거나 차단하지 않습니다.

참고

각 항목별 예외 목록은 각각 최대 30개까지 추가할 수 있습니다.

참고

각 항목에서 사용 안 함을 선택한 경우에는 예외 목록을 설정할 수 없습니다.

실행 방법

1 환경 설정>네트워크 보안>행위 기반 침입 차단에서 **행위 기반 침입 차단 사용**을 선택합니다.

2 알려지지 않은 프로토콜 드라이버/이상 트래픽/ARP 스푸핑에서 탐지나 차단을 선택하고 **예외 목록**을 누릅니다.

3 선택한 항목의 예외 목록 설정 창이 나타납니다.

알려지지 않은 프로토콜 드라이버 예외 목록

❖ 추가: 알려지지 않은 프로토콜 드라이버 공격에 대한 예외를 목록에 추가할 수 있습니다. 추가를 누르면, <알려지지 않은 프로토콜 드라이버 추가>가 나타납니다.

- 프로토콜 이름: 탐지된 프로토콜 목록에서 예외로 설정할 프로토콜을 선택합니다. 탐지된 프로토콜이 없는 경우 **탐지된 내역이 없습니다.** 라는 메시지가 표시됩니다.
- 프로세스 이름: 모든 프로세스를 선택하거나 프로세스 목록 중에서 선택할 수 있습니다. **찾아보기**를 누르면, 프로세스를 직접 선택할 수 있습니다.

❖ 삭제: 예외 목록에 추가된 프로토콜과 프로세스를 선택한 후 **삭제**를 누르면 해당 내용을 목록에서 삭제합니다. 삭제한 내용에 대해서는 더 이상 예외 규칙을 적용하지 않습니다.

❖ 예외 프로토콜: 사용자가 추가한 예외 프로토콜 이름을 표시합니다.

❖ 예외 프로세스: 사용자가 추가한 예외 프로세스 이름을 표시합니다.

이상 트래픽 예외 목록

❖ 추가: 이상 트래픽 탐지나 차단의 예외를 목록에 추가할 수 있습니다. 추가를 누르면, <IP 주소 추가/수정>에서 이상 트래픽 예외 IP 주소를 설정할 수 있습니다. 설정된 IP 주소에서 이상 트래픽이 발생하더라도 탐지하거나 차단하지 않습니다.

❖ 수정: 이상 트래픽 예외 IP 주소 목록에서 대상을 선택하고 수정을 누르면, <IP 주소 추가/수정>에서 IP 주소를 수정할 수 있습니다.

❖ 삭제: 이상 트래픽 예외 IP 주소 목록에서 대상을 선택하고 삭제를 누르면, 이상 트래픽 예외 목록에서 삭제합니다.

❖ 이상 트래픽 예외 IP 주소: 사용자가 추가한 이상 트래픽 탐지나 차단의 예외 규칙을 적용할 IP 목록을 표시합니다.

ARP 스푸핑 공격 예외 목록

❖ 추가: ARP 스푸핑 공격에 대한 예외를 목록에 추가할 수 있습니다. 추가를 누르면, <ARP 스푸핑 공격 예외 게이트웨이 추가/수정>이 나타납니다.

- 게이트웨이 이름: 게이트웨이 이름을 입력합니다.
- 게이트웨이 IP 주소: 게이트웨이 IP 주소를 입력합니다.

- 게이트웨이 MAC 주소: 게이트웨이 MAC 주소를 입력합니다.

❖ 수정: 예외 목록에 추가한 게이트웨이 정보를 수정합니다.

❖ 삭제: 예외 목록에 추가된 게이트웨이를 선택한 후 **삭제**를 누르면 해당 내용을 목록에서 삭제합니다. 삭제한 내용에 대해서는 더 이상 예외 규칙을 적용하지 않습니다.

❖ 게이트웨이 이름: 사용자가 추가한 게이트웨이 이름을 표시합니다.

❖ IP 주소: 사용자가 추가한 게이트웨이의 IP 주소를 표시합니다.

❖ MAC 주소: 사용자가 추가한 게이트웨이의 MAC 주소를 표시합니다.

개인 방화벽

개인 방화벽을 사용하면 네트워크 규칙과 프로그램 규칙에 따라 허가하지 않은 인터넷 연결을 차단하여 PC를 안전하게 유지할 수 있습니다. 개인 방화벽은 다른 PC에서 사용자의 PC로 들어오는 데이터와 사용자의 PC에서 다른 PC로 나가는 데이터를 제한합니다. 허가없이 PC에 접근하여 악성코드를 유포하는 공격자의 침입이나 내 PC의 정보가 외부로 유출되는 것을 예방할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **네트워크 보안>개인 방화벽**을 선택합니다.

개인 방화벽 사용 여부 선택

❖ 개인 방화벽 사용: 개인 방화벽 기능을 사용하도록 설정합니다. 개인 방화벽을 사용하면 네트워크 규칙과 프로그램 규칙에 따라 사용자 PC를 보호합니다.

❖ 프로파일: 프로파일은 개인 방화벽의 정책 세트로 사용할 프로파일 이름을 선택하면 네트워크 규칙과 프로그램 규칙에 정의되지 않은 네트워크 연결 요청이 발생할 경우 프로파일에 설정된 내용에 따라 처리합니다.

❖ 프로파일 설정:<프로파일 설정>에서는 네트워크 규칙과 프로그램 규칙에 정의되지 않은 네트워크 연결에 대한 처리 방법 등을 설정할 수 있습니다.

참고

프로파일은 사용자 PC에서 기본적으로 1개를 설정할 수 있으며, V3 관리 프로그램인 APC를 사용하는 경우 APC 관리자가 설정한 프로파일을 적용할 수도 있습니다. APC 관리자가 설정한 프로파일은 프로파일 목록에 APC Policy로 표시됩니다.

프로파일 설정

프로파일 설정에서는 개인 방화벽 규칙의 네트워크 규칙과 프로그램 규칙에 정의되지 않은 네트워크 연결 요청에 대한 처리 방법을 설정할 수 있습니다.

실행 방법

1 환경 설정>네트워크 보안>개인 방화벽에서 **개인 방화벽 사용**을 선택합니다.

2 **프로파일 설정**을 누릅니다.

3 <프로파일 설정>이 나타나면, 프로파일 이름, 처리 방법, 기타 옵션을 설정합니다.

- 프로파일 이름: 프로파일 이름을 입력합니다.
- 처리 방법: 규칙에 정의되지 않은 네트워크 연결 요청이 발생했을 경우 처리 방법을 설정할 수 있습니다.
- 기타 옵션: 처리 방법과 더불어 네트워크 연결 요청시 확인할 내용을 설정할 수 있습니다.

처리 방법

❖ 규칙에 정의되지 않은 네트워크 연결: 네트워크 규칙과 프로그램 규칙에 정의되지 않은 네트워크 연결 요청이 발생한 경우 해당 요청에 대한 처리 방법을 선택합니다.

- 허용: 네트워크 연결을 허용합니다.
- 차단: 네트워크 연결을 차단합니다.
- 사용자 알림 후 결정: 규칙에 정의되지 않은 네트워크 연결이 발생했을 경우 알림 창이 나타납니다. 알림 창에서 사용자가 직접 연결을 허용하거나 차단할 수 있습니다.

- 신뢰 프로그램 자동 연결: 신뢰 프로그램 목록에 등록된 프로그램이 네트워크 연결을 요청한 경우에는 자동으로 연결을 허용합니다. 신뢰 프로그램 자동 연결을 사용하면 신뢰 프로그램은 자동 연결하지만, 신뢰 프로그램에 등록되지 않은 프로그램이 네트워크 연결을 요청할 경우에는 알림 창이 나타납니다.
- 자동 결정: 신뢰 프로그램이 네트워크 연결을 요청한 경우에는 자동으로 허용하고, 신뢰 프로그램이 아닌 경우에는 자동으로 연결을 차단합니다.
- 디지털 서명 확인: 실행 파일의 디지털 서명 정보를 확인하여 서명이 유효한 경우에만 연결합니다.
- 클라우드 평판 기반 실행 차단 사용: 안랩 클라우드 서버의 평판 정보를 확인하여 평판 정보가 정상인 경우에만 연결합니다.

참고

디지털 서명 확인이나 클라우드 평판 기반 실행 차단은 신뢰 프로그램 자동 연결이나 자동 결정을 선택한 경우에 필요한 옵션입니다. 따라서, 신뢰 프로그램 자동 연결이나 자동 결정을 선택한 경우 디지털 서명 확인이나 클라우드 평판 기반 실행 차단 사용 옵션을 최소 1개 이상 선택해야 합니다.

기타 옵션

❖ 파일 고유 정보 확인: 파일의 고유 정보인 해시 값을 확인하여 프로그램 파일이 변조되었는지 확인합니다.

❖ 포트 숨김(스텔스 포트) 사용: 특정 포트를 사용하는 프로그램의 취약점을 이용한 포트 스캐닝 공격을 예방할 수 있는 기능으로 사용자 PC에서 연결을 허용한 포트 외에는 외부에서 사용자 PC에 연결할 수 없도록 합니다.

네트워크 규칙

네트워크 규칙은 IP 주소, 프로토콜, 포트 번호, 연결 방향으로 구성된 개인 방화벽 규칙으로 네트워크를 통해 다른 PC와 데이터를 주고 받는 것을 연결하거나 차단하도록 규칙을 설정할 수 있습니다. 개인 방화벽의 네트워크 규칙을 이용하면 믿을 수 있는 PC만 데이터를 주고 받는 것을 허용하고 해킹과 같은 위험을 막아 PC를 보호할 수 있습니다.

실행 방법

1 환경 설정>네트워크 보안>개인 방화벽에서 **개인 방화벽 사용**을 선택합니다.

2 네트워크 규칙에서 **규칙 목록**을 누릅니다.

3 <네트워크 규칙 목록>이 나타나면 규칙을 추가, 수정, 삭제하거나 우선 순위를 변경할 수 있습니다.

- 추가: 네트워크 규칙 목록에 규칙을 추가합니다. 추가를 누르면,<네트워크 규칙 추가>에서 규칙을 추가할 수 있습니다.
- 수정: 네트워크 규칙 목록에서 항목을 선택하고 수정을 누르면 규칙을 수정할 수 있습니다.
- 삭제: 네트워크 규칙 목록에서 항목을 선택하고 삭제를 누르면 규칙 목록에서 해당 항목을 삭제합니다.
- 규칙 이름: 사용자가 입력한 네트워크 규칙의 이름을 표시합니다.
- 네트워크 연결: 네트워크 연결에 대한 연결/차단 여부를 표시합니다.
- 사용 여부: 해당 규칙의 사용 여부를 표시합니다.
- 설명: 네트워크 규칙에 대해 사용자가 입력한 설명입니다.
- 우선 순위 변경: 네트워크 규칙 목록에서는 규칙의 표시 순서가 적용 우선 순위입니다. 우선 순위를 변경할 항목을 선택하고 **위로/아래로**를 누르면 해당 규칙의 우선 순위를 높이거나 낮춥니다.

네트워크 규칙 추가

네트워크 규칙 추가에서는 새로운 네트워크 규칙을 만들어 규칙 목록에 추가할 수 있습니다. 네트워크 규칙은 네트워크 연결, 프로토콜 및 포트, IP 주소, 규칙 종류의 순서대로 설정해야 합니다.

네트워크 연결

❖ 네트워크 연결: 네트워크에 연결할 때 규칙에서 설정한 IP 주소, 프로토콜, 포트를 사용한 요청에 대해 연결하거나 차단하도록 설정합니다.

❖ 연결 방향: 모두, 들어오기, 나가기를 선택할 수 있습니다.

- 모두: 연결한 IP 주소와 데이터를 주고 받는 들어오기와 나가기를 모두 연결하거나 차단합니다.
- 들어오기: 연결한 IP 주소에서 데이터를 받는 것을 연결하거나 차단합니다.

- 나가기: 연결한 IP 주소로 데이터를 보내는 것을 연결하거나 차단합니다.

프로토콜 및 포트

❖ 프로토콜 종류: 통신 프로토콜에서 연결하거나 차단할 프로토콜을 선택합니다.

- TCP: TCP 프로토콜을 이용한 통신을 연결하거나 차단합니다.
- UDP: UDP 프로토콜을 이용한 통신을 연결하거나 차단합니다.
- ICMP: ICMP 프로토콜을 이용한 통신을 연결하거나 차단합니다. ICMP를 선택한 경우, **ICMP 종류**를 눌러 종류를 선택할 수 있습니다.

❖ 포트 범위: 설정한 포트로 통신을 할 때 연결하거나 차단할 포트를 설정합니다.

- 모든 포트: 모든 포트를 연결하거나 차단합니다.
- 사용자 지정 포트: 사용자가 입력한 포트에 대해서만 연결하거나 차단합니다. 사용자 지정 포트를 선택하면, 로컬 포트나 원격 포트를 입력할 수 있습니다.
- 로컬 포트: 내 PC의 포트 번호를 입력합니다.
- 원격 포트: 내 PC가 아닌 연결을 요청하는 상대방의 포트 번호를 입력합니다.

IP 주소

❖ IP 범위: 규칙을 적용할 주소를 지정합니다.

- 모든 IP 주소: 모든 IP 주소에 규칙을 적용합니다.
- 사용자 지정 IP 주소(최대 8개): 사용자가 입력한 IP 주소에만 규칙을 적용합니다. 사용자 지정 IP 주소는 최대 8개까지 입력할 수 있습니다.
- 추가: 사용자 지정 IP 주소를 선택한 경우 추가를 눌러 IP 주소를 설정합니다. 추가를 누르면,<IP 주소 추가/수정>에서 규칙을 적용할 IP 주소를 설정할 수 있습니다.
- 수정: 사용자 지정 IP 주소 목록에서 항목을 선택하고 수정을 누르면, <IP 주소 추가/수정>에서 IP 주소를 수정할 수 있습니다.
- 삭제: 사용자 지정 IP 주소 목록에서 항목을 선택하고 삭제를 누르면, 사용자 지정 IP 주소 목록에서 선택한 항목을 삭제합니다.

규칙 종류

- ❖ 규칙 이름: 규칙의 이름을 입력합니다. 규칙 이름은 중복되지 않게 입력해야 하며 63자까지 입력할 수 있습니다.
- ❖ 설명: 규칙에 대한 설명을 입력합니다. 설명은 127자까지 입력할 수 있습니다.
- ❖ 로그 남김: 해당 규칙이 적용되면 로그를 기록합니다. 단, UDP 프로토콜에 대해서는 로그를 남기지 않습니다.

ICMP 종류 선택

ICMP는 네트워크 연결 상태를 확인하거나 연결 중에 발생한 오류 정보를 전달하는 프로토콜로 전송할 ICMP 메시지의 종류를 선택합니다. 기본값으로 모두 선택되어 있습니다.

- ❖ 에코 요청(8): ICMP Echo Request를 전송합니다. 패킷을 목적지에 전송할 수 있는지 확인합니다.
- ❖ 에코 응답(0): 에코 요청에 대한 응답으로 ICMP Echo Reply를 전송합니다. 에코 응답이 정상적으로 확인되면 패킷을 전송할 수 있습니다.
- ❖ 타임 스탬프 요청(13): ICMP Timestamp Request를 전송합니다.
- ❖ 타임 스탬프 응답(14): 타임 스탬프 요청에 대한 응답으로 ICMP Timestamp Reply를 전송합니다.
- ❖ 정보 요청(15): ICMP Information Request를 전송합니다.
- ❖ 정보 응답(16): 정보 요청에 대한 응답으로 ICMP Information Reply를 전송합니다.
- ❖ 주소 마스크 요청(17): ICMP Address Mask Request를 전송합니다.
- ❖ 주소 마스크 응답(18): 주소 마스크 요청에 대한 응답으로 ICMP Address Mask Reply를 전송합니다.
- ❖ 도메인 이름 요청(37): ICMP Domain Name Request를 전송합니다.
- ❖ 도메인 이름 응답(38): 도메인 이름 요청에 대한 응답으로 ICMP Domain Name Reply를 전송합니다.
- ❖ ICMPv6 목적지 접근 불가(1): 목적지에 접근하지 못해 전달하지 못한 경우 Host Unreachable를 전송합니다.
- ❖ ICMPv6 패킷 크기 초과(2): 패킷의 크기를 초과하여 전송하지 못한 경우 Protocol Unreachable를 전송합니다.
- ❖ ICMPv6 시간 초과(3): 패킷이 목적지에 전달되기 전에 시간이 초과한 경우 Port Unreachable를 전송합니다.

❖ ICMPv6 에코 요청(128): Echo Request를 전송합니다. 패킷을 목적지에 전송할 수 있는지 확인합니다.

❖ ICMPv6 에코 응답(129): 에코 요청에 대한 응답으로 Echo Reply를 전송합니다. 에코 응답이 정상적으로 확인되면 패킷을 전송할 수 있습니다.

❖ ICMPv6 홈 주소 요청(144): Home Agent Address Discovery Request를 전송합니다.

❖ ICMPv6 홈 주소 응답(145): 홈 주소 요청에 대한 응답으로 Home Agent Address Discovery Reply를 전송합니다.

프로그램 규칙

프로그램 규칙을 사용하면 PC에 설치된 프로그램이 네트워크에 연결하는 것을 허용하거나 차단하도록 설정할 수 있습니다. 프로그램 규칙은 PC에 설치된 프로그램이 패치나 업데이트 등의 목적으로 인터넷 연결을 필요로 할 때 해당 연결을 허용할지 차단할지를 사용자가 선택하는 기능입니다. 올바른 프로그램 제작사에서 제공하는 프로그램 관련 패치나 업데이트는 사용자에게 필요하지만, 악의적인 목적을 가진 프로그램의 네트워크 연결 요청은 사용자 정보를 몰래 유출하거나 악성코드를 설치하기 위한 용도로 악용될 수 있습니다.

프로그램 규칙은 악의적인 용도로 네트워크 연결을 요청하는 프로그램의 네트워크 연결을 차단하기 위해 네트워크 연결이 필요한 프로그램에 대해서는 연결을 허용하고 네트워크 연결을 필요로 하지 않는 프로그램에 대해서는 연결을 차단하도록 설정하여 PC를 보호하는데 도움을 줄 수 있습니다.

실행 방법

1 환경 설정>네트워크 보안>개인 방화벽에서 **개인 방화벽 사용**을 선택합니다.

2 프로그램 규칙에서 **추가**를 누르면 나타나는 <프로그램 규칙 추가>에서 프로그램 규칙을 설정할 수 있습니다.

- 추가: <프로그램 규칙 추가>에서 프로그램 규칙을 설정합니다.
- 수정: 프로그램 규칙 목록에서 항목을 선택하고 수정을 누르면 규칙을 수정할 수 있습니다.
- 삭제: 프로그램 규칙 목록에서 항목을 선택하고 삭제를 누르면 규칙 목록에서 해당 항목을 삭제합니다.
- 프로그램 이름: 규칙을 적용하는 프로그램의 이름을 표시합니다.

- 네트워크 연결: 프로그램의 네트워크 허용에 대한 허용/차단 여부를 표시합니다.
- 사용 여부: 해당 규칙의 사용 여부를 표시합니다.
- 설명: 프로그램 규칙에 대해 사용자가 입력한 설명입니다.

프로그램 규칙 추가

프로그램 규칙 추가에서는 새로운 프로그램 규칙을 만들어 규칙 목록에 추가할 수 있습니다. 프로그램 규칙은 규칙을 적용할 프로그램 선택, 네트워크 연결, 규칙 종류의 순서대로 설정해야 합니다.

프로그램 선택

❖ 찾아보기: 규칙을 적용할 프로그램을 찾아보기를 눌러 선택합니다. 프로그램을 선택하면 입력란에 선택한 프로그램의 경로와 파일 이름이 자동 입력됩니다.

❖ 제작사: 선택한 프로그램의 제작사 정보가 표시됩니다.

❖ 디지털 서명: 선택한 프로그램 파일의 디지털 서명의 유효성을 표시합니다.

❖ 파일 설명: 선택한 프로그램 파일에 대한 설명을 표시합니다.

❖ 파일 고유 정보: 선택한 프로그램 파일에 대한 해시 정보를 표시합니다.

네트워크 연결

❖ 네트워크 연결: 프로그램이 네트워크에 연결을 요청할 때 연결하거나 차단하도록 설정합니다.

- 허용: 프로그램의 네트워크 연결을 허용합니다.
- 차단: 프로그램의 네트워크 연결을 차단합니다.
- 사용자 지정: 프로그램이 네트워크 연결을 요청할 경우 사용자가 설정한 네트워크 규칙에 따라 처리합니다.

참고

사용자 지정을 선택하면 프로그램의 네트워크 규칙을 별도로 설정할 수 있습니다.

네트워크 규칙

네트워크 연결에서 사용자 지정을 선택한 경우에는 선택한 프로그램에 대한 네트워크 규칙을 설정할 수 있습니다.

- ❖ 추가: 네트워크 규칙 목록에 규칙을 추가합니다. 추가를 누르면, <네트워크 규칙 추가/수정>에서 규칙을 추가할 수 있습니다.
- ❖ 수정: 네트워크 규칙 목록에서 항목을 선택하고 수정을 누르면 규칙을 수정할 수 있습니다.
- ❖ 삭제: 네트워크 규칙 목록에서 항목을 선택하고 삭제를 누르면 규칙 목록에서 해당 항목을 삭제합니다.
- ❖ 규칙 이름: 사용자가 입력한 네트워크 규칙의 이름을 표시합니다.
- ❖ 네트워크 연결: 네트워크 연결에 대한 허용/차단 여부를 표시합니다.
- ❖ 우선 순위 변경: 네트워크 규칙 목록에서는 규칙의 표시 순서가 적용 우선 순위입니다. 우선 순위를 변경할 항목을 선택하고 위로/아래로를 누르면 해당 규칙의 우선 순위를 높이거나 낮춥니다.
- ❖ 규칙에 정의되지 않은 연결: 프로그램의 네트워크 규칙에 정의되지 않은 프로그램이 네트워크 연결을 요청할 때 처리하는 방법을 선택합니다.
  - 허용: 프로그램의 네트워크 연결을 허용합니다.
  - 차단: 프로그램의 네트워크 연결을 차단합니다.

참고

프로그램의 네트워크 규칙에 대한 자세한 설명은 네트워크 규칙의 네트워크 규칙 추가를 참고하십시오.

규칙 종류

- ❖ 규칙 이름: 규칙의 이름을 입력합니다. 규칙 이름은 중복되지 않게 입력해야 하며 63자까지 입력할 수 있습니다.
- ❖ 설명: 규칙에 대한 설명을 입력합니다. 설명은 127자까지 입력할 수 있습니다.
- ❖ 로그 남김: 해당 규칙이 적용되면 로그를 기록합니다.

Active Defense

Active Defense 설정

Active Defense는 알려지지 않은 위협에 능동적으로 대처하기 위해 위협을 가시화하고 판단 근거를 제공하여 적극적인 방어 기회를 제공합니다. Active Defense를 사용하면 PC에서 실행되는 프로그램이 의심 행위를 하는지를 판단하고 점검합니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **Active Defense>Active Defense 설정**을 선택합니다.

ASD 네트워크 설정

ASD 네트워크 설정에서는 클라우드 서비스를 담당하는 ASD(AhnLab Smart Defense) 서버의 악성코드 데이터베이스를 활용하여 파일의 악성 여부를 검사하고 클라우드 서버에 보고되지 않은 새로운 파일을 발견했을 때는 해당 파일을 서버로 전송하여 실시간으로 분석하고 결과를 사용자에게 알려줍니다.

❖ ASD 네트워크 참여: 클라우드 기반의 ASD 네트워크에 참여하면, 클라우드 서버에 보고되지 않은 새로운 악성코드를 발견했을 경우 해당 파일을 ASD 클라우드 서버에 전송하고 분석 결과를 사용자에게 실시간으로 알려줍니다.

❖ ASD 사용권 계약 보기: ASD 네트워크 참여 및 데이터 수집 동의서가 나타납니다. 내용을 확인하고 해당 내용에 동의하는 경우 ASD 네트워크 참여를 해 주십시오.

- Active Defense 사용: Active Defense 기능을 사용합니다.

참고

ASD 네트워크에 참여하는 사용자가 많을수록 악성코드 데이터베이스의 정보가 증가하여 악성코드 감염으로 인한 위협을 감소시키는데 많은 도움이 됩니다.

참고

Active Defense는 PC 실시간 검사 작동 시에만 사용할 수 있습니다. PC 실시간 검사를 사용하지 않으면, Active Defense 사용을 선택했더라도 기능이 작동하지 않습니다.

사용자 지정 파일 관리

사용자가 신뢰하는 파일은 신뢰 파일로 추가하고, 사용을 원하지 않는 파일이거나 악성코드로 의심되는 파일에 대해서는 차단 파일로 추가하여 해당 파일의 실행을 차단할 수 있습니다.

- ❖ 신뢰 추가: **신뢰 추가**를 눌러 <열기>가 나타나면 신뢰 목록에 추가할 파일을 선택하고 **열기**를 누릅니다. 등록한 파일은 신뢰/차단 파일 목록에 상태 값이 신뢰로 표시됩니다.
- ❖ 차단 추가: **차단 추가**를 눌러 <열기>가 나타나면 차단 목록에 추가할 파일을 선택하고 **열기**를 누릅니다. 등록한 파일은 신뢰/차단 파일 목록에 상태 값이 차단으로 표시됩니다.
- ❖ 삭제: 신뢰/차단 파일 목록에 등록된 파일을 선택하고 **삭제**를 누르면, **선택한 항목을 삭제하시겠습니까?** 라는 메시지가 나타납니다. **예**를 누르면 선택한 파일을 목록에서 삭제합니다.

참고

사용자 지정 파일 관리에서 신뢰/차단 파일은 최대 300개까지 추가할 수 있습니다.

참고

차단 파일로 추가된 파일을 정밀 검사나 PC 실시간 검사에서 발견한 경우 해당 파일을 삭제합니다.

클라우드 자동 분석

클라우드 자동 분석은 알려지지 않은 위협을 발견했을 경우 해당 행위를 하는 파일을 클라우드 자동 분석 서버로 전송하여 악성 여부를 분석하고 결과를 실시간으로 알려주는 기능입니다.

- ❖ 클라우드 자동 분석 사용: 클라우드 자동 분석을 사용하면, 정밀 검사나 PC 실시간 검사에서 알려지지 않은 위협을 발견했을 경우 클라우드 자동 분석 서버로 발견된 파일을 자동 전송하여 분석을 의뢰합니다. 분석 결과는 검사 종료 시에 사용자에게 알려줍니다.

기타 설정

사용자 설정

사용자 설정에서는 V3 시작 화면 설정과 데이터 보관을 위한 보관 기간 등을 설정할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **기타 설정>사용 환경>사용자 설정** 탭을 선택합니다.

시작 화면 설정

V3의 시작 화면을 사용자가 선택할 수 있습니다.

❖ HOME 화면: V3의 시작 화면을 HOME 화면으로 표시합니다. HOME 화면에서는 보안 상태, 업데이트, 빠른 검사, 클라우드 현황 정보를 간략히 표시합니다. 시작 화면의 기본값입니다.

❖ 고급 화면: V3의 시작 화면을 고급 화면으로 표시합니다. 고급 화면에서는 보안 센터와 정밀 검사, 네트워크 보안, 도구 등의 개별 기능에 접근할 수 있습니다.

참고

HOME 화면에 대한 정보는 HOME>화면 구성을 참고하시고, 시작 화면을 고급 화면으로 설정한 경우에는 보안 센터>화면 구성을 참고하십시오.

보관 기간 설정

V3를 실행한 후 발생하는 각종 로그와 백업 파일을 저장할 디스크 공간 크기와 기간을 설정합니다.

❖ 진단 로그 보관 기간(4~365일): PC 검사와 클라우드 진단에서 발생한 로그를 보관하는 기간을 설정합니다. 진단 로그 보관 기간은 4~365일 사이에서 입력할 수 있습니다.

❖ 이벤트 로그 보관 기간(4~365 일): V3 의 각종 기능을 실행할 때 발생하는 이벤트 로그를 보관하는 기간을 설정합니다. 이벤트 로그 보관 기간은 4~365 일 사이에서 입력할 수 있습니다.

❖ 검역소 보관 기간(4~365 일): 악성코드에 감염된 백업 파일을 보관하는 검역소에 파일을 보관하는 기간을 설정합니다. 검역소 보관 기간은 4~365 일 사이에서 입력할 수 있습니다.

잠금 설정

허가받지 않은 사용자가 일부 기능을 임의로 중지하거나 환경 설정을 변경하는 것을 방지하고 V3 를 제거하는 것을 방지하기 위해 설정된 비밀번호를 입력한 후에 해당 기능을 이용할 수 있도록 합니다.

❖ 잠금 설정 사용: 잠금 설정을 사용합니다. 잠금 설정을 사용하면, 비밀번호 입력 후 V3 프로그램 삭제나 환경 설정을 변경할 수 있습니다.

비밀번호 설정

잠금 설정에서 사용할 비밀번호를 설정합니다.

❖ 비밀번호 입력: 비밀번호를 입력합니다. 비밀번호는 영문자, 숫자, 특수 문자를 모두 포함하여 10~30 자 사이에서 입력해야 합니다.

❖ 비밀번호 확인: 입력한 비밀번호를 다시 입력합니다.

⚠ 주의

비밀번호를 분실하면 복구할 수 없으므로 주의하십시오.

비밀번호 확인

잠금 설정에서 비밀번호를 설정한 후에 V3 프로그램을 삭제하거나 환경 설정 값을 변경하려고 하면 다음과 같은 비밀번호 입력 창이 나타납니다.

❖ 비밀번호: 잠금 설정에서 설정한 비밀번호를 입력하십시오.

잠금 예외 설정

설정한 항목에 대해서는 잠금 설정의 예외를 적용하여 비밀번호를 입력하지 않아도 설정 내용을 변경할 수 있습니다.

❖ 예약 검사 설정: 예약 검사 설정은 잠금 설정 상태에서 비밀번호를 입력하지 않아도 사용할 수 있습니다.

❖ 개인 방화벽의 네트워크 규칙 설정: 개인 방화벽의 네트워크 규칙 설정은 잠금 설정 상태에서 비밀번호를 입력하지 않아도 사용할 수 있습니다.

❖ 개인 방화벽의 프로그램 규칙 설정: 개인 방화벽의 프로그램 규칙 설정은 잠금 설정 상태에서 비밀번호를 입력하지 않아도 사용할 수 있습니다.

탐색기 메뉴

Windows 탐색기에서 디스크 드라이브/폴더/파일을 선택하고 마우스 오른쪽을 누르면 탐색기 메뉴를 사용할 수 있습니다. 탐색기 메뉴를 설정하면, V3를 직접 실행하지 않아도 탐색기에서 파일을 검사하거나 파일 완전 삭제를 실행하고 선택한 파일의 분석 보고서를 확인할 수 있어 편리합니다.

❖ 탐색기 검사: 검사할 드라이브나 폴더, 파일에서 마우스 오른쪽 버튼을 누르면 탐색기 검사를 실행할 수 있습니다. 탐색기 검사를 선택하면, 선택한 대상에 대한 악성코드 감염 여부를 검사하고 치료합니다.

❖ 파일 완전 삭제: 검사할 폴더나 파일에서 마우스 오른쪽 버튼을 누르면 파일 완전 삭제를 실행할 수 있습니다. 파일 완전 삭제를 실행하면, 선택한 대상을 복구 불가능한 상태로 삭제합니다.

❖ 파일 분석 보고서 열기: 파일 분석 보고서를 확인하고 싶은 파일에서 마우스 오른쪽 버튼을 누르면 파일 분석 보고서 열기를 실행할 수 있습니다. 파일 분석 보고서는 선택한 파일에 대한 버전 정보, 프로그램 제작사 관련 정보, 클라우드 정보 등을 확인할 수 있습니다.

참고

파일 분석 보고서의 클라우드 관련 정보는 사용자 PC가 네트워크에 연결된 경우에만 내용이 표시됩니다.

알림 설정

알림 창 표시 상황을 사용자가 직접 선택하고 악성코드 진단/치료나 업데이트와 같은 특정 이벤트가 발생했을 때 사용자에게 알려주는 알림 상황을 선택할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **기타 설정>사용 환경>알림 설정** 탭을 선택합니다.

알림 설정에서 설정할 수 있는 옵션

- ❖ 전체 화면 모드일 때 알림 창 표시하지 않기: 파워포인트에서 프리젠테이션을 하거나 워드 같은 프로그램에서 전체 화면 모드를 사용할 때 알림 창 발생을 금지합니다. 전체 화면 모드 상태에서 악성코드를 발견한 경우 모두 자동으로 치료하며 방화벽은 사용자에게 확인하지 않고 모두 차단 모드로 동작하여 사용자의 현재 작업을 방해하지 않습니다.
- ❖ 풍선 도움말 알림 창 표시: 사용자에게 일회성 정보를 알려줄 때 나타나는 풍선 도움말의 표시 여부를 선택합니다.
- ❖ 선택한 상황에 알림 창 표시: 알림 설정에서 사용자가 선택한 상황이 발생했을 때 작업 표시줄에 알림 창을 보여줍니다. 알림 창에서는 발생한 상황에 따라 차단한 내용이나 감염된 악성코드 이름 등을 확인할 수 있습니다. 알림 상황은 **설정**을 누르면 나타나는 <알림 상황 설정>에서 선택할 수 있습니다.

알림 상황 설정

알림 설정의 선택한 상황에 알림 창 표시를 선택하고 설정을 누르면 알림 상황을 설정할 수 있습니다. 알림 상황은 V3에서 발생하는 다양한 이벤트에 대하여 사용자에게 세부 내용을 알림 창으로 알려주고 필요한 경우 사용자 선택을 요청합니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **기타 설정>사용 환경>알림 설정** 탭을 선택합니다.

3 선택한 상황에 **알림 창 표시**를 선택하고 **설정**을 누르면 <알림 상황 설정>이 나타납니다.

알림 상황 설정

사용자에게 필요한 알림 상황을 선택할 수 있습니다. 선택한 알림 상황이 발생했을 경우 알림 창이 화면에 표시됩니다.

전체

❖ 전체: 전체 알림 상황을 모두 선택하거나 선택을 모두 해제합니다.

PC 보안

❖ 악성코드를 진단/치료한 경우 알림: V3가 악성코드를 발견하거나 치료한 경우에 알림 창이 나타납니다.

❖ 불필요한 프로그램(PUP)를 진단/치료한 경우 알림: 검사 대상에서 불필요한 프로그램을 검사 대상으로 선택한 후 V3가 불필요한 프로그램을 진단하거나 치료한 경우에 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>PC 실시간 검사>검사 대상>설정>불필요한 프로그램(PUP) 프로그램 선택
- 관련 옵션: 환경 설정>정밀 검사/예약 검사>검사 대상>설정>불필요한 프로그램(PUP) 프로그램 선택

❖ 클라우드 평판이 낮은 프로그램이 실행된 경우 알림: 클라우드 평판이 낮은것으로 알려진 프로그램이 실행된 경우에 알림 창이 나타납니다. 클라우드 평판 점수는 최초 발견 날짜, 사용자 수, 의심 행위 수에 대한 정보를 종합적으로 수집하여 계산합니다.

- 관련 옵션: 환경 설정>PC 실시간 검사>클라우드 평판 기반 실행 차단 사용 선택

❖ 악성코드 치료 시 PC를 다시 시작해야 할 때 알림: 감염된 악성코드를 치료하기 위해 PC를 다시 시작해야 할 때 알림 창이 나타납니다. 악성코드를 치료를 위해 PC를 지금 다시 시작하거나 다시 시작하지 않도록 선택할 수 있습니다.

❖ V3 제품 파일이 감염되어 진단/치료한 경우 알림: V3 제품을 실행 할 때 V3 제품 파일이 감염되었는지를 검사하고 치료할 때 나타납니다.

- 관련 옵션: 환경 설정>고급 설정>고급 검사>V3 제품 보호 선택

❖ 행위 기반 진단 중 의심 행위 발견 알림: 행위 기반 진단 중에 의심 행위를 하는 파일을 발견했을 경우 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>Active Defense>Active Defense 설정>Active Defense 사용 선택

❖ V3 제품 보호 알림: V3 제품 보호 대상인 파일, 프로세스, 레지스트리에 접근하는 프로세스를 탐지했을때 나타납니다.

- 관련 옵션: 환경 설정>고급 설정>고급 검사>V3 제품 보호 선택

❖ 예약 검사 실행 알림: 사용자가 선택한 주기에 예약 검사를 실행할 때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>PC 검사 설정>예약 검사>예약 검사 사용 선택

❖ 중요 시스템 파일 접근 차단 알림: 마스터 부트 레코드나 중요 시스템 파일에 대한 접근을 차단했을 때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>고급 설정>고급 검사>중요 시스템 파일 보호 선택

❖ 무결성 검사 중 손상된 파일이 있을 때 알림: PC 시작할 때 V3 파일의 무결성을 검사하고 손상된 파일이 있을때 나타납니다.

- 관련 옵션: 환경 설정>고급 설정>고급 검사>PC 시작할 때 V3 무결성 검사 선택

❖ 클라우드 자동 분석 요청을 위해 파일 전송할 때 알림: 안랩 클라우드 서버에 정보가 없는 파일을 탐지하고 해당 파일을 클라우드 자동 분석 서버로 전송할 때 나타납니다.

- 관련 옵션: 환경 설정>Active Defense 설정>클라우드 자동 분석 사용 선택

❖ 사용자 지정 차단 파일을 차단한 경우 알림: Active Defense의 사용자 지정 파일 관리에 추가한 차단 파일을 차단했을 때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>Active Defense 설정>ASD 네트워크 참여>Active Defense 사용>사용자 지정 파일 관리>차단 파일 추가

네트워크 보안

❖ 악성 사이트 접근 차단 알림: 홈페이지 변조를 통해 악성코드를 다운로드하게 하는 악성 사이트의 접속을 차단했을때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단 선택

❖ 피싱 사이트 접근 차단 알림: 피싱 사이트 접근을 차단했을 때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단>피싱 사이트 차단 선택

❖ 불필요한 사이트(PUS) 접근 차단 알림: 불필요한 사이트 접근을 차단했을 때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단>불필요한 사이트(PUS) 차단 선택

❖ 사용자 지정 사이트 접근 차단 알림: 사용자가 차단 사이트로 등록한 사이트에 접근했을 때 알림 창이 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>웹 보안>유해 사이트 차단>사용자 지정 사이트 관리>차단 추가에서 입력한 사이트

❖ 네트워크 침입 차단 알림: 네트워크를 통해 사용자 PC에 침입 시도를 탐지했거나 V3가 공격을 탐지한 시점에 공격자가 연결된 세션을 종료했을때 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>침입 차단>네트워크 침입 차단>네트워크 침입 차단 사용 선택

❖ 행위 기반 침입 차단 알림: 알려지지 않은 프로토콜 드라이버의 실행을 탐지했을 때 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>침입 차단>행위 기반 침입 차단>행위 기반 침입 차단 사용 선택

❖ 프로그램이 네트워크 연결을 시도할 때 알림: 방화벽 규칙에 정의되지 않은 프로그램이 네트워크 연결을 시도할 때 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>개인 방화벽>개인 방화벽 사용 선택

❖ 개인 방화벽 규칙 업데이트가 필요한 경우 알림: 방화벽에 추가된 프로그램의 파일이 변경되었을 때 나타납니다.

- 관련 옵션: 환경 설정>네트워크 보안>개인 방화벽>개인 방화벽 사용 선택

업데이트

❖ 업데이트를 실패한 경우 알림: 업데이트를 실패했을 때 나타납니다.

❖ 업데이트가 필요한 경우 알림: 최신 엔진으로 업데이트해야할 때 나타납니다.

업데이트 설정

V3가 최신 보안 위협으로 부터 사용자 PC를 지키려면 악성코드 및 클라우드, 네트워크 보안에 필요한 관련 정보 파일을 항상 최신 버전으로 업데이트해야 합니다. 업데이트 설정에서는 좀 더 편리하게 업데이트하기 위해 자동 업데이트를 선택하거나 사용자가 선택한 시간에 업데이트할 수 있도록 업데이트 시간을 예약할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **기타 설정>사용 환경>업데이트 설정** 탭을 선택합니다.

업데이트 방법 설정

업데이트 방법 설정에서는 자동 업데이트와 예약 업데이트 사용 여부를 선택할 수 있습니다.

❖ 자동 업데이트 사용(권장): PC 부팅 후 5~30분 사이에 업데이트 서버에 접속하여 업데이트 여부를 확인합니다.

- 자동 업데이트 주기(1~24시간): PC 부팅 이후 자동 업데이트 주기에 따라 업데이트 여부를 확인하여 업데이트합니다.

❖ 예약 업데이트 사용: 일정한 주기와 시간을 설정하여 예약한 시간에 업데이트를 자동으로 실행합니다.

- 매일: 매일 지정한 시간에 업데이트를 실행합니다.
- 매주: 매주 지정한 요일과 시간에 업데이트를 실행합니다.
- 매월: 매월 지정한 날짜와 시간에 업데이트를 실행합니다.
- 한 번만: 지정한 날짜와 시간에 업데이트를 한 번만 실행합니다.

⚠주의

새로 발견되는 악성코드를 치료하기 위해서는 최신 엔진 파일로 사용자 PC를 주기적으로 검사할 것을 권장합니다. 업데이트 불편 해소와 악성코드로 인한 피해를 최소화하려면 자동 업데이트를 항상 사용하고 업데이트 주기는 가장 짧은 간격을 유지하십시오.

업데이트 고급 설정

❖ 업데이트할 때 V3 패치 파일도 다운로드: 최신 엔진을 업데이트할 때 V3 프로그램의 변경 사항이 반영된 패치 파일을 다운로드합니다.

❖ 업데이트 파일 무결성 검사: 다운로드한 업데이트 파일의 손상 여부나 감염 여부를 검사합니다.

❖ 업데이트 실패한 경우 재시도 횟수(1~99): 업데이트를 실패했을 경우 자동으로 재시도하는 횟수를 설정합니다. 재시도 횟수는 1~99회까지 설정할 수 있습니다.

❖ Stable 엔진 사용: 업데이트할 때 최신 엔진을 다운로드하지 않고 최신 버전 이전의 버전으로 업데이트합니다.

서버 설정

서버 설정에서는 V3에서 업데이트 시 인터넷을 연결할 때 프록시 서버 사용 여부와 분석 보고서를 출력하기 위한 통신 포트를 설정할 수 있습니다.

실행 방법

1 V3 실행 후 환경 설정을 선택합니다.

2 **기타 설정>사용 환경>서버 설정** 탭을 선택합니다.

프록시 서버 설정

업데이트를 위해 인터넷에 연결할 때 프록시 서버를 사용해야하는 경우 설정합니다.

❖ 프록시 서버 사용: 업데이트할 때 프록시 서버를 통해 인터넷에 연결합니다.

- 서버 주소: 프록시 서버의 주소를 입력합니다. 프록시 서버 주소는 IP 주소나 도메인 이름을 입력할 수 있으며, 최대 1024자까지 입력할 수 있습니다.
- 포트 번호(1~65535): 프록시 서버에서 사용하는 포트 번호를 입력합니다. 포트 번호는 1~65535 사이에서 입력할 수 있습니다.
- 로그인 ID: 프록시 서버의 로그인 ID를 입력합니다.
- 비밀번호: 프록시 서버의 로그인 비밀번호를 입력합니다.

보고서 서버 설정

V3는 파일 분석 보고서와 사이트 분석 보고서를 출력하기 위해 사용자 PC에 보고서 서버를 설치합니다. 보고서 서버 설정에서는 보고서 서버의 통신 포트 번호를 수정할 수 있습니다. 보고서 통신 포트는 V3가 자동으로 설정하지만, 사용자 PC에서 해당 포트 번호를 이미 사용 중인 경우에는 보고서 서버 설정에서 사용하지 않는 포트 번호로 직접 설정해야 합니다.

❖ 포트 번호(1~65535): 수정할 보고서 통신 포트를 입력합니다. 기본값은 1235입니다.

참고

보고서 서버의 포트 번호는 기존에 사용 중인 포트 번호와 충돌하지 않는다면 V3에서 설정한 기본값대로 사용하고, 포트 충돌이 발생할 경우에 보고서 서버 설정에서 포트 번호를 변경할 것을 권장합니다.

색인

ㅎ

A

C

E

F

I

O

S

T

V

W